Exchange 2003 VSS Backup Solution for IBM System Storage™ DS8000/DS6000 and Symantec Backup Exec 11d

Configuration and Best Practices

David West, David Hartman
IBM System and Technology Group
August 2007

Table of Contents

Authors

David West[i], David Hartman[ii],

Created on: December 10, 2006

Latest update: August 1, 2007, Revision 2.0

Trademarks

IBM Systems and Technology Group
Route 100
Somers, NY 10589

Produced in the U.S.A.

DISCLAIMER

Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. The information contained in this document is current as of the initial date of publication only, and IBM shall have no responsibility to update such information. Product data is subject to change without notice. This information could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or programs(s) at any time without notice. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM program or product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectually property rights, may be used instead. It is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

Performance data for IBM and non-IBM products and services contained in this document was derived under specific operating and environmental conditions. The actual results obtained by any party implementing and such products or services will depend on a large number of factors specific to such party's operating environment and may vary significantly. IBM makes no representation that these results can be expected or obtained in any implementation of any such products or services.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR INFRINGEMENT.

The provision of the information contained herein is not intended to, and does not grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

Executive Summary

Customers rely on Microsoft Exchange, SQL Server, and various internet/intranet applications as key business applications. Even short periods of unexpected downtime can have a serious impact. The capability of backing up and restoring data quickly and consistently is essential. The problems in backing up large amounts of data, such as backup jobs frequently overflowing their backup window, and having open file and application issues, led to the development of snapshots.

The capability to take snapshots has been around for several years. Snapshots allow administrators to “snap” a copy of data while allowing applications to continue running. Applications are paused just long enough to allow the disk system to create the snap copy. These volumes could then be mounted to another server for backing up to various storage devices. Snapshots, however, depended on tight hardware and software compatibility which was often problematic, inducing errors that were difficult to track and resolve. In addition, the vendors needed to support various versions of SQL Server, Microsoft® Exchange, Windows® Server, and myriad other applications.

Microsoft developed VSS (Volume Shadow Copy Service) as a common framework to resolve these issues. Available in Windows Server 2003, software and hardware vendors now have a common interface model for generating snapshots. The VSS framework specifies how three distinct components should interact. The three different components are the VSS requestor, writer, and provider. The requestor is the backup software, such as the Backup Exec Agent. The writer is the application software such as SQL Server or Exchange Server that pause to allow the snapshots to be taken. The provider is the specific hardware/software combination that generates the snapshot volume, in this case, the IBM System Storage™ DS Hardware Provider.

The Importance of Exchange VSS Solutions

Businesses have grown to rely on access to their Microsoft Exchange servers to address the increasing demands of mobile computing, global business and electronic commerce. They depend on Exchange e-mail, group scheduling, and calendars for critical business communication and key business processes. E-mail also supports vital applications needed for functions such as workflow, collaboration, and knowledge management. According to Microsoft, nearly 45 percent of business-critical information is housed in e-mail and e-mail-attached documents.

Cost of Downtime

When a critical system like an Exchange server goes down, data, productivity, and money may be lost. For a typical business that has 500 active users on an Exchange server, if access to that server is lost for two hours the company may experience a productivity loss of as much as 1000 employee hours, which can equate to tens of thousands of dollars. That does not consider other losses, such as missed communications from partners, damaged customer relations, or simply lost deals.

Target Environment

The IBM System Storage™ DS6000 and DS8000 series storage arrays target medium to large-size businesses seeking enterprise level reliability, availability, and serviceability (RAS), combined with support of advanced copy features such as FlashCopy®, and Metro/Global Mirror®. In a large environment, it is not uncommon to have multiple DS6000 and DS8000 arrays deployed in a complimentary fashion. The DS8000 series is designed to scale to the needs or the largest enterprise data centers.

Customers deploying these arrays for Exchange-based solutions will typically have installations that range from several servers hosting a thousand or more users on a DS6000 at a single site, to fully-loaded DS8000 multi-node arrays hosting tens of thousands of users. Usually, the latter types of deployments include geographically dispersed clusters with multi-site data replication enabled.

The current version of Backup Exec 11d for Microsoft Exchange does not include instant recovery capabilities, however future releases may support this functionality.

During lab testing the average recovery time for a single Storage Group with a 50GB database was ~ 20 minutes (vs. ~ 5 minutes for instant recovery). While faster than tape-based recovery methods, these restore times should be considered against RTOs and service level agreements (SLAs) if applicable.

In many cases, production recovery requests are for individual mailboxes, rather than entire databases or storage groups. With the introduction of Backup Exec Granular Recovery Technology, Symantec enables faster RTOs for mailbox or item level restores, which can be restored from VSS backups.

IBM System Storage™ DS8000 Series

Created specifically for medium and large enterprises, the IBM System Storage™ DS8000 series offers high-capacity storage systems that are designed to deliver a generation-skipping leap in performance, scalability, resiliency and value.

The DS8000 series is designed to provide exceptional performance while adding virtualization capabilities that can help you allocate system resources more effectively and better control application quality of service (QoS). The DS8000 series also offers powerful functions that are designed to help protect data from unforeseen events and maintain data availability, which can benefit businesses that must have round the clock access to information.

- Exceptional flexibility and scalability. The current physical storage capacity of the DS8000 series system can range from 1.1TB to 512TB, and it has an architecture designed to scale to over a petabyte.
- Significant availability enhancements. IBM System Storage FlashCopy®, Global and Metro Mirror functions, and streamlined configuration and management capabilities through the easy-to-use IBM DS Storage Manager are just some of the many additional advanced features of the DS8000 series.
- Innovative design creates impressive performance. With 4Gb fibre technology, the DS8000 models are as much as seven times faster than the IBM TotalStorage Enterprise Storage Server® (ESS) Model 800.
- Utilizing IBM POWER5+™ processor technology, the DS8000 series delivers the first use of the IBM Virtualization Engine™, which is designed to bring to disk storage systems the logical partition flexibility usually reserved for enterprise-class servers.

Additional information regarding the DS8000 can be found at:

http://www-03.ibm.com/systems/storage/disk/ds8000/index.html

IBM System Storage™ DS6000 Series

The IBM System Storage DS6000 series is a member of the family of DS products and is built upon 2 Gbps fibre channel technology that provides RAID-protected storage with advanced functionality, scalability, and increased availability capabilities.

The DS6000 series is designed to offer a high reliability and performance-orientated midrange storage solution through the use of hot-swappable redundant RAID controllers in a space efficient modular design. The DS6000 series provides storage sharing and consolidation for a wide variety of operating systems and mixed server environments.

The DS6000 series is designed to offer high scalability while maintaining excellent performance. With the base DS6800 (Model 1750-511), you can install up to 16 disk drive modules (DDMs).

If you want to connect more than 16 disks, simply use the optional DS6000 expansion enclosures (Model 1750-EX1) that allow a maximum of 128 DDMs per storage system and provide a maximum physical storage capability of 38.4TB (FC), or 64TB (FATA).

The small, 3U form-factor allows for maximum density with a minimal footprint. Available in a 19-inch rack mountable package with optional modular expansion enclosures of the same size, the DS6000 offers capacity to help address your growing business needs, while conserving precious space, power, and cooling resources.

The DS6000 series addresses business efficiency needs through its heterogeneous connectivity, high performance and manageability functions, thereby helping to reduce total cost of ownership.

The DS6000 series offers the following major features:

- PowerPC® 750GX processors
- Dual active controllers are designed to maintain operations through the use of two processors that form a pair to back up one another
- A selection of 2 GB Fibre Channel (FC) & FATA disk drives, including 73, 146, 300, & 500GB sizes with speeds of 10,000 or 15,000 revolutions per minute (RPM)
- 2 GB Fibre Channel and FICON host attachments of up to 8 ports, which can be configured with an intermix of Fibre Channel Protocol (FCP) and FICON

- Fibre Channel Arbitrated Loop (FC-AL), point-to-point (FC-P2P), and switched-fabric (FC-SW) host connectivity topologies supported
- Battery backed mirrored cache
- Redundant power and cooling systems
- Disaster recovery and advanced Copy Services solutions

You can also view the DS6000 e-learning overview from the DS6000 Storage Manager Welcome page or at:

http://www-.ibm.com/support/docview.wss?rs=1112&uid=ssg1S7001165

The e-learning overview provides an animated presentation about installation and configuration, service and support, and management tasks.

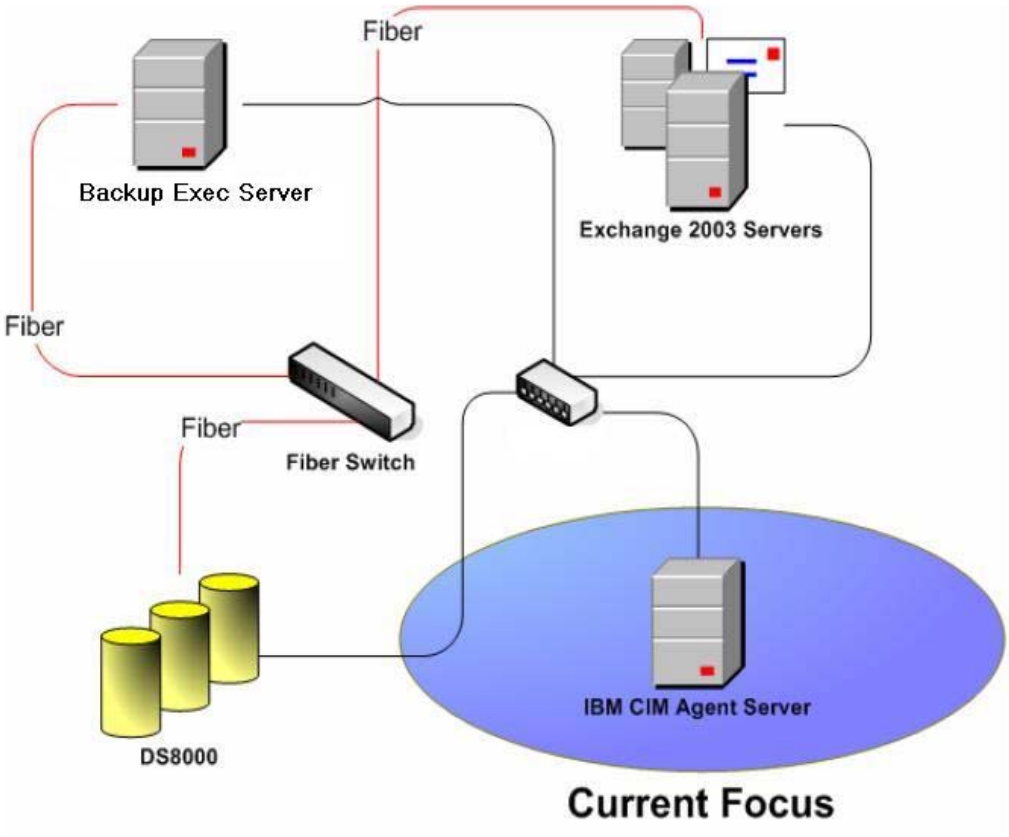
Additional information regarding the DS6000 can be found at:

http://www-03.ibm.com/systems/storage/disk/ds6000/index.html

Installing CIM Agent for Windows

The CIM Agent for DS Open (API) is a middleware application that provides a CIM-compliant interface for applications that require it, or can make use of it. Elsewhere you may see this (and other interfaces into the DS Open framework) referred to generically as the DS Open API. The agent code provides a CIM API into the IBM System Storage DS8000 & DS6000.

This section includes an overview of the installation process and instructions for installing and configuring the CIM agent on a Windows 2000 or later operating system. It should be noted that although this solution places the CIM agent on a separate Windows 2003 server, that is not a requirement. The CIM agent can be installed on any server (including the Exchange or Backup Exec servers), as well as on Linux® & AIX® hosts.



Installation Overview for Windows

This section provides an overview of the installation and configuration of the CIM agent on a Windows Server 2003 system. Ensure that you have sufficient knowledge of how to administer a Windows Server 2003 system before you install the CIM agent. Also, you should be familiar with the commands that you use during installation and configuration of the CIM agent. The following list of installation and configuration tasks is in the order in which they should be performed:

1. Before you install the CIM agent for Windows, verify the hardware and software requirements.
2. If you are managing ESS storage units, you must install the prerequisite ESS CLI level 2.4.0.236 (or higher) software. The ESS CLI must be installed first because the CIM agent sets the path information in shell scripts for you based on the location of the ESS CLI. The CIM agent installation wizard checks your system for the existence of the ESS CLI, and the wizard displays a warning message if ESS CLI is not installed. For ESS CLI installation instructions, see the *IBM TotalStorage Enterprise Storage Server Command-Line Interfaces User's Guide*. This guide is available at:

   http://publibfp.boulder.ibm.com/epubs/pdf/f2bcli04.pdf

   Attention: If you are upgrading from a previous version of the CIM agent, you must upgrade the ESS CLI software to the new required minimum level of 2.4.0.236.
3. You can choose to install the CIM agent either in graphical mode with the help of an installation wizard or in unattended mode (also known as silent mode), which involves customizing a response file and issuing a command.
4. Verify the CIM agent Windows installation.
5. Configure the CIM agent for Windows. You may want to revisit the configuration section in the future as you add, change, or delete CIMOM authentication and storage unit information.
6. Verify the connection to your storage unit.
7. Optionally, remove the CIM agent. You only need to perform this optional task if you get errors during installation verification or if the CIM agent did not set the environment variables.

Installing the CIM Agent on Windows

This section includes the steps to install the CIM agent in your Windows environment.

You must satisfy all prerequisites before you begin the CIM agent installation.

After the completion of installation, you must verify the installation of the CIM agent. Before you install the CIM agent on Windows, verify that your system meets all of the hardware and software requirements.

1. Log on to your system as the local administrator.
2. Insert the CIM agent CD into the CD-ROM drive. The CIM agent program should start within 15 - 30 seconds if you have autorun mode set on your system. If the LaunchPad window does not open, perform the following steps:
    a. Use a Command Prompt or Windows Explorer to change to the Windows directory on the CD.
    b. If you are using a Command Prompt window, type: `LaunchPad`
    c. If you are using Windows Explorer, double-click on the **LaunchPad.bat** file.

    Note: If you are viewing the folder in Windows Explorer with the option selected to hide file extensions for known file types, find the LaunchPad file with the file type of MS-DOS Batch File.

The following options are displayed when the LaunchPad window opens:

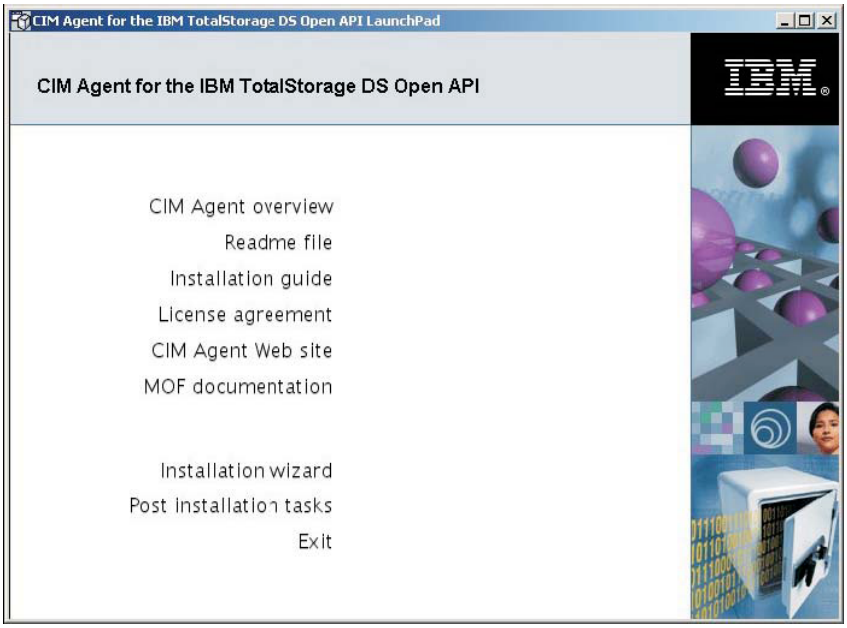


Figure 1: The Launchpad Window

CIM Agent overview: Offers information about the CIM agent.

Readme file: Offers any last minute product information that did not make it into the installation guide.

Installation guide: Offers instructions on how to install the CIM agent.

License agreement: Offers information about the license for the CIM agent.

CIM Agent Web site: Offers information from the product Web site.

MOF Documentation: Offers information about MOF documentation.

Installation wizard: Starts the CIM agent installation program.

Post installation tasks: Offers information about configuring users and storage unit communication.

Exit: Exits the CIM agent LaunchPad program.

> **Note:** Before beginning the installation, click the **Readme** file from the LaunchPad window or open the **README.txt** file located in the doc or Windows directory on the CIM agent CD to check for information that might supersede the information in this guide.

From the Launchpad window, click **Installation wizard** to start the installation.

Note: The LaunchPad window remains open (behind the wizard) during the installation and returns to the foreground when the installation is complete. You can click **Exit** to close the LaunchPad.

1. There might be a slight delay while the software loads on your system. After the software loads a DOS prompt window opens to display the following message:

```
Initializing InstallShield Wizard... Preparing Java (tm) Virtual
Machine……..
```

2. The Welcome window is displayed. Make a note of the recommended documents to read prior to installation. Click **Next** to continue, or click **Cancel** to exit the installation.

3. Read and accept the License Agreement, and then click **Next**.

4. If the installation wizard detects a prior installation of the CIM agent, the Product Installation Check window opens. Check the Preserve Configuration check box if you want to preserve your configuration settings. Follow any specific instructions in the window. For example, the figure below shows a warning to stop running services. Once you have followed all instructions, select Next.

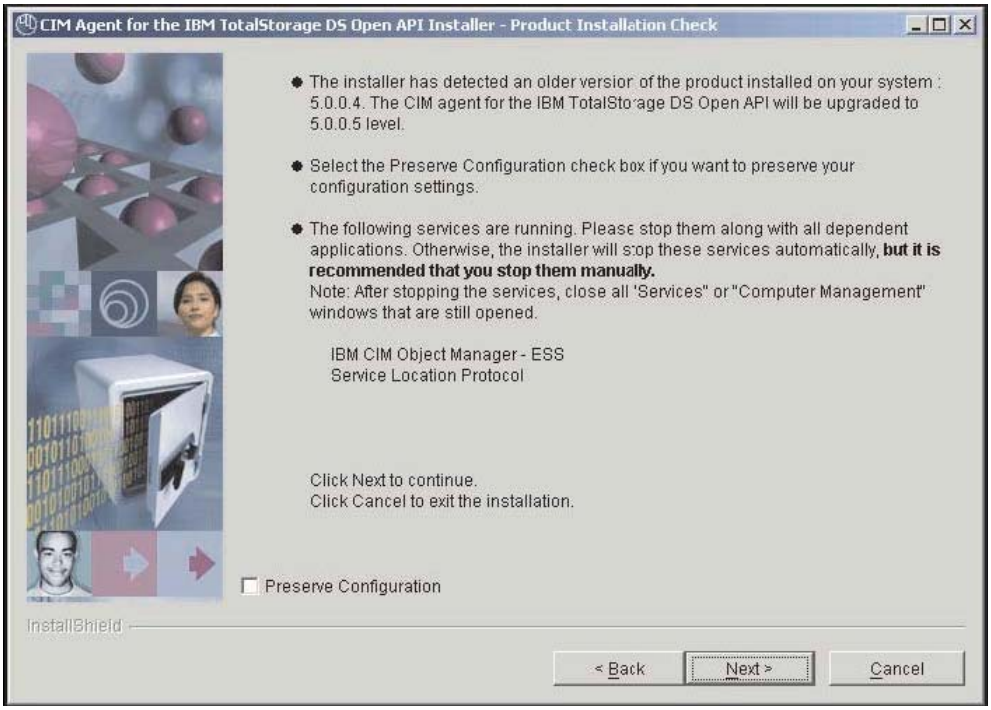


Figure 2: Product Installation Check window

5. The IBM ESS CLI Check window opens. The wizard verifies that you have the IBM ESS CLI installed if you are managing ESS storage units.

Note: The window is not displayed if you have the required version of the ESS CLI already installed.b

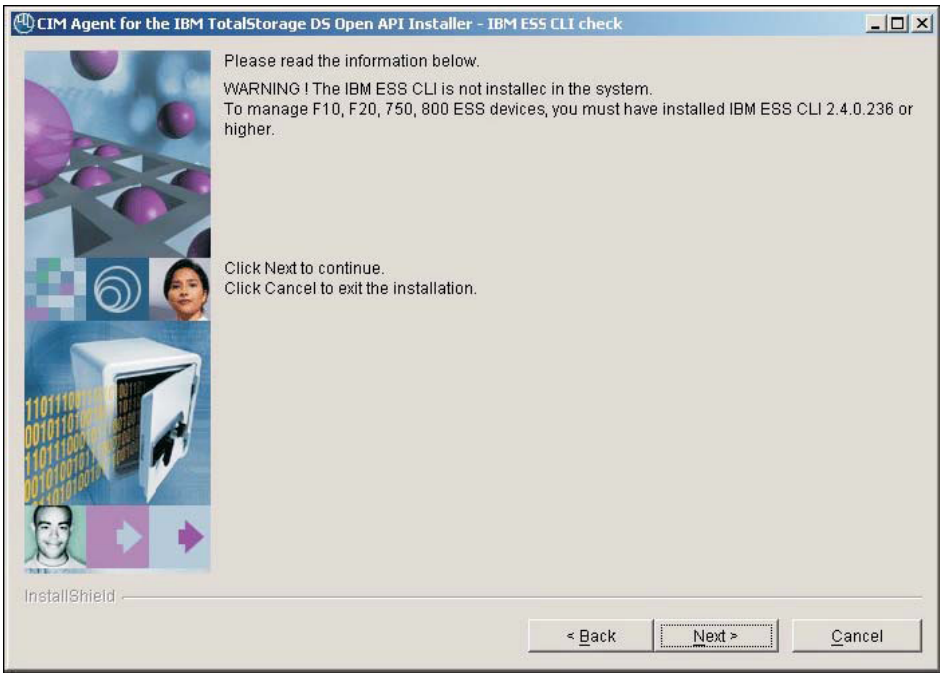


Figure 3: IBM ESS CLI window

6. The Destination Directory window is displayed. Click **Next** to accept the default directory for the installation files, or click **Browse** to select a different directory. Click **Next**.

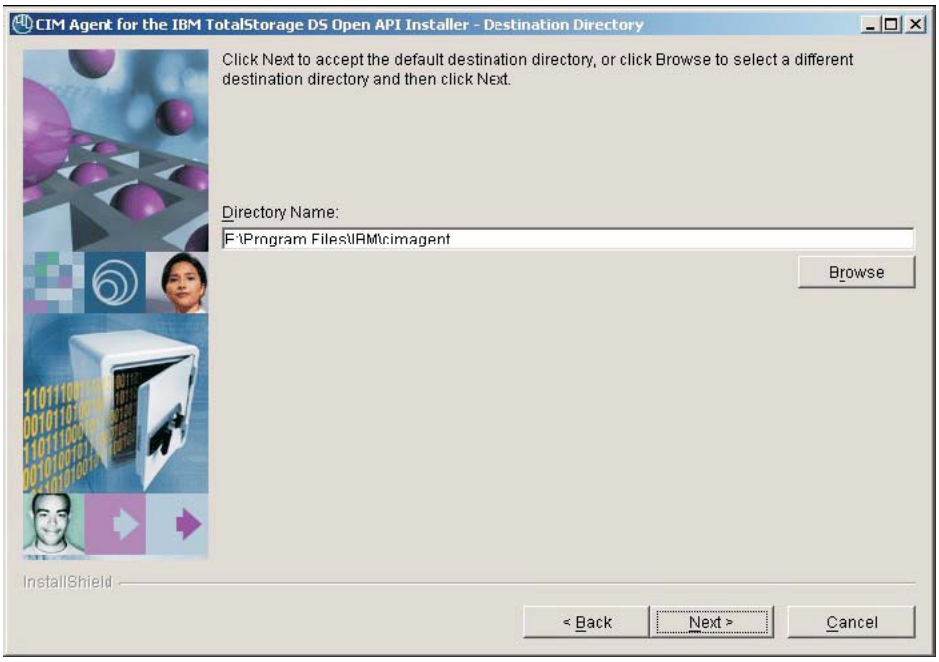


Figure 4: Destination Directory window

Please note:

- The Destination Directory window is displayed *only* if a version of CIM agent is not already installed. Otherwise, the CIM agent is reinstalled or upgraded to the same install location.
- If the program detects insufficient space for the CIM agent installation in the chosen destination, an error message is displayed. You can free some space on the destination drive and then click Next or you can stop the installation program by clicking Cancel. You can also click **Back**, and choose another destination directory for the product.

7. The Updating CIMOM Port window opens. Click **Next** to accept the default port. If the default port is the same as another port already in use, modify the default port and click **Next**. Use the following command to check which ports are in use:

   ```
   netstat -a
   ```

   Either accept **HTTPS** as the communication protocol or select another protocol.

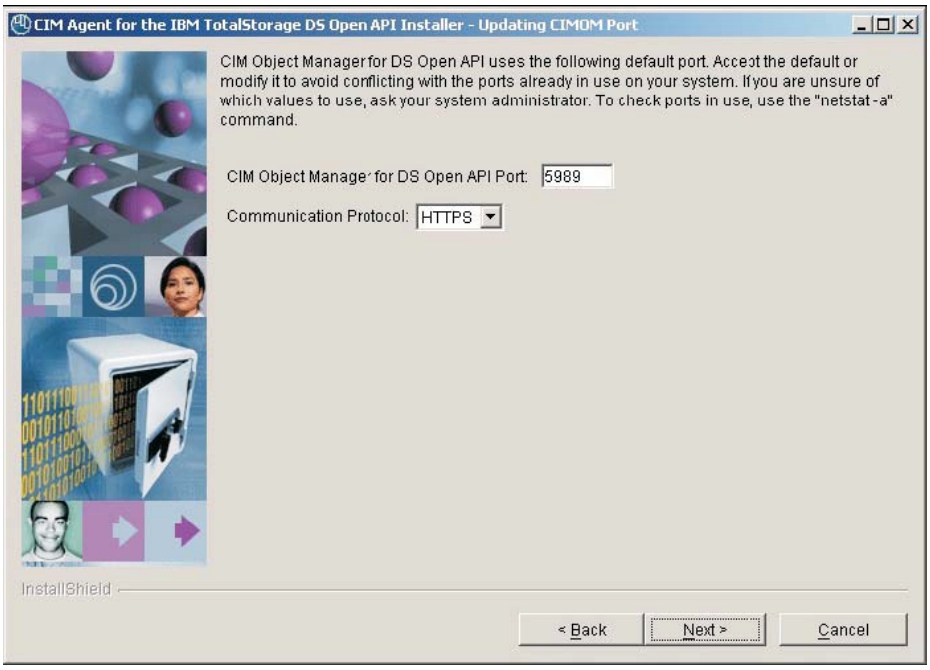


Figure 5: Update CIMOM Port window

8. The Installation Confirmation window opens. Click **Install** to confirm the installation location and file size. You can click Cancel to exit the installation wizard or go back to the previous window by clicking **Back**.

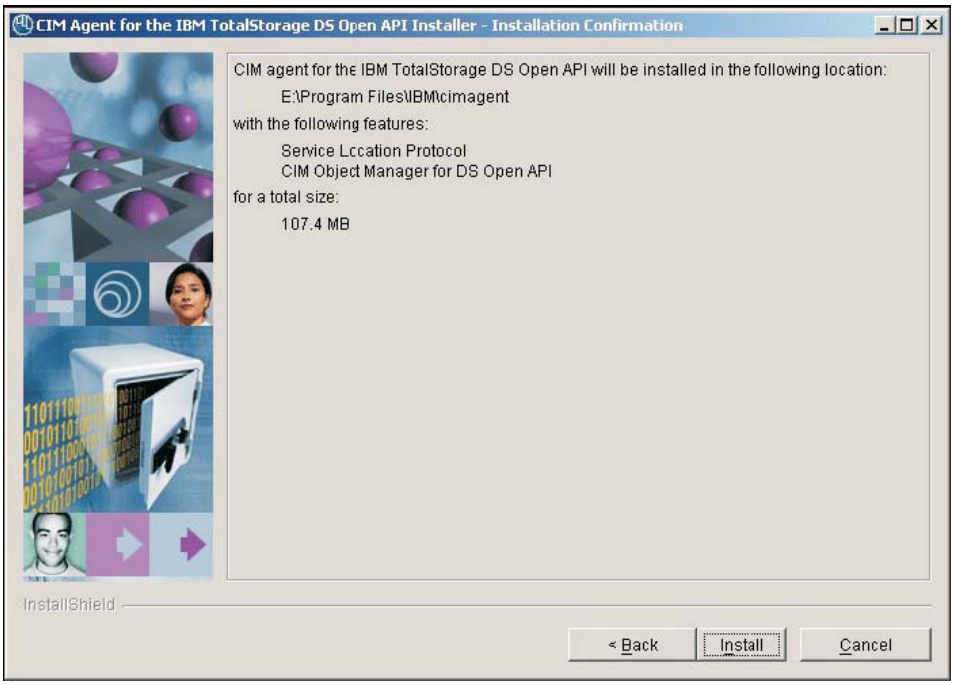


Figure 6: Installation Confirmation window

9. Installation usually takes 3 - 10 minutes depending on the configuration of your system. You can click Cancel to exit the installation wizard.

   Note: If you click **Cancel**, a window opens asking you to confirm the cancellation of the installation wizard. If you confirm the cancellation by clicking **Yes**, the information entered or selected in previous windows is not saved. You will need to start the installation again from the beginning.

10. After the Installation Progress window closes, the Finish window is displayed. You can view the post installation tasks by clicking the **View post installation tasks** checkbox, or you can deselect the checkbox and continue with the post installation tasks. Click **Finish** to exit the installation wizard.

    Note: Before proceeding, you might want to review the log file for any possible error messages. The log file is located in xxx\logs\install.log, where xxx is the destination directory where the CIM agent for Windows is installed. The install.log contains a trace of the installation actions.

11. Exit the LaunchPad program by clicking **Exit** on the LaunchPad window. If you have not done so already, continue with the post installation tasks for the CIM agent using the instructions in the following sections.

    Note: Typically, you do not need to restart your system during or after the installation of the CIM agent. If the installation wizard determines that a restart is necessary, restart your system. After you restart the system, the installation wizard will continue with the installation of the CIM agent.

Verifying the CIM Agent Installation on Windows

This task verifies that your CIM agent is installed correctly on your Windows server. Perform the following steps to verify your CIM agent:

1. Verify the installation of the Service Location Protocol (SLP).

   a. Verify that SLP is started. Select **Start → Settings → Control Panel**. Double-click the **Administrative Tools** icon, and then double-click the **Services** icon.

   b. Find Service Location Protocol in the Services window list. For this component, the Status column should be marked Started and the Startup Type column should be marked Manual. If those conditions are not met, right-click on the SLP and select Start from the pop-up menu. Wait for the Status column to be changed to Started.

c. Do not close the Services window because you will also use it to verify the CIM object manager (CIMOM) service.

2. Verify the installation of the CIM agent.

   a. Verify that the CIMOM service is started. If you closed the Services window, select **Start → Settings → Control Panel**. Double-click the **Administrative Tools** icon, and then double-click the **Services** icon.

   b. Find **CIM Object Manager - DS Open API** in the Services window list. For this component, the Status column should be marked **Started** and the Startup Type column should be marked **Automatic**. If those two conditions are not met, right click on the **CIM Object Manager - DS Open API** and select **Start** from the pop-up menu. Wait for the Status column to change to **Started**.

   c. Close the **Services** window.

   d. Close the **Administrative Tools** window.

If you are able to perform all of the verification tasks successfully, the DS CIM agent has been successfully installed on your Windows system. Next, perform the required configuration tasks.

Configuring the CIM Agent for Windows

This task configures the CIM agent after it has been successfully installed. This section repeats the instructions in the Post Installation Tasks option that you open from the LaunchPad window.

You can also use the ***modifyconfig*** command to change the configuration of some of the parameters that were configured during installation. You can change the CIM agent port value, protocol (HTTP/HTTPS), and enable or disable the debug option.

Steps:

Perform the following steps to configure the CIM agent:

1. Ping each ESS and DS that the CIM agent will manage by typing the following command:

    a. Open a command prompt window and issue a **ping** command; for example:

    ```
    ping 9.11.111.111
    ```

    where 9.11.111.111 is and ESS or DS IP address.

    b. Check that you can see reply statistics from the IP address. The following is example output:

    ```
    Pinging 9.11.111.111 with 32 bytes of data: Reply from
     9.11.111.111: bytes=32 time<10ms TTL=255

    Reply from 9.11.111.111: bytes=32 time<10ms TTL=255

    Reply from 9.11.111.111: bytes=32 time<10ms TTL=255

    Reply from 9.11.111.111: bytes=32 time<10ms TTL=255
    ```

If you see other messages that indicate that the request has timed out, see your Network Administrator for help on establishing network connectivity before you configure storage units.

2. Configure the CIM agent for each ESS or DS which the CIM agent can access. Change directories into the CIM agent directory; for example: C:\Program Files\IBM\cimagent and type the following command to start the interactive **setdevice** tool to identify servers to the CIMOM:

    ```
    setdevice
    ```

    a. For each ESS, type the following command:

```
>>>addess 9.11.111.111 essuser esspass
```

where:

- *9.11.111.111* represents the IP address of the ESS.
- *essuser* represents an ESS storage manager user name.
- *esspass* represents the password for the user name.

The following is example output:

```
A provider entry for IP 9.11.111.111 successfully added
```

b. Type the following command for each ESS configured for Copy Services or for each DS server the CIM agent will access:

```
>>> addessserver 9.11.111.111 essuser esspass
9.22.222.222
```

where:

- *9.11.111.111* represents the IP address of the ESS or DS server
- *essuser* represents a user name for the server.
- *esspass* represents the password for the user name.
- *9.22.222.222* represents the alternate IP address of the server.

Note: Specifying an alternate IP address is optional. The alternate IP address is used if a connection cannot be made using the primary IP address. The following is example output:

```
An essserver entry for IP 9.11.111.111 successfully
added
```

3. Repeat step for each additional storage unit that you want to configure.
4. Close the **setdevice** interactive session by typing **exit**.
5. Once you have defined all the servers, you must stop and restart the CIMOM to make the CIMOM initialize the information for the servers. Because the CIMOM collects and caches the information from the defined servers at startup time, the starting of the CIMOM might take a longer period of time the next time you start it.

Perform the following steps to use the Windows Start Menu facility to stop and restart the CIMOM:

a. Stop the CIMOM by selecting **Start → Programs → CIM agent for IBM DS Open API → Stop CIMOM service**. A command prompt window opens to track the stoppage of the CIMOM.

Note: You might see an error message pop-up window that is labeled "*java.exe - Application Error*". You must click OK to close that window to continue.

If the CIMOM has stopped successfully, the following message is displayed:

```
The CIM Object Manager for DS Open API service was
stopped successfully. Press any key to close the command
prompt window.
```

b. Restart the CIMOM by selecting **Start → Programs → CIM agent for IBM DS Open API → Start CIMOM service**. A command prompt window opens to track the progress of the CIMOM start process. The restarting of the CIMOM can take a while because it is connecting to the defined servers and is caching that information for future use. If the CIMOM has started successfully, the following message is displayed:

```
The CIM Object Manager for DS Open API service was
started successfully.

Press any key to close the command prompt window.
```

6. Use the **setuser** interactive tool to configure the CIMOM for the users with authority to use the CIMOM.

   Note: The users you configure to use the CIMOM are uniquely defined to the CIMOM software and have no required relationship to operating system user names, the DS Storage Manager user names, or the Copy Services user names.

   Upon installation of the CIM agent, the provided default user name is "superuser" with a default password of "**passw0rd**". The first time that you use the **setuser** tool, you must use this user name and password combination. Once you have defined other user names, you can start the **setuser** command by specifying other defined CIMOM user names.

   Note: The CIMOM must be running before you can use the **setuser** command.

   a. Open a Command Prompt window and change directory to the CIM agent directory; for example:

```
C:\Program Files\IBM\cimagent
```

b. Type the following command at the command prompt to start the **setuser** interactive session to identify users to the CIMOM:

```
setuser -u superuser -p passw0rd
```

c. Type the following command in the **setuser** interactive session to define new users:

```
>>>adduser cimuser cimpass
```

where:

- *cimuser* represents the new user name that can access the CIM agent CIMOM
- *cimpass* represents the password for the new user name that can access the CIM agent CIMOM

The following is example output:

```
An entry for user cimuser successfully added where
cimuser is the new user name.
```

7. Repeat step 6c for each additional user name that you want to configure.
8. You can change the default password for “superuser” by starting the **setuser** command and by providing a user name and password. Issue the **setuser** interactive session command to change the password for the superuser:

```
>>>chuser superuser newpasswd
```

where *newpasswd* is the new password for the superuser.

You can also delete the superuser by issuing the following **setuser** interactive session command:

```
>>>rmuser superuser
```

9. Close the **setuser** interactive session by typing **exit**.

Note: Unlike the **setdevice** actions, you are *not* required to stop and restart the CIMOM to make the **setuser** actions take effect.

If you were able to perform all of the configuration tasks successfully, the CIM agent has been successfully installed and configured on your Windows system.

Configuring the CIM Agent to run in Unsecure Mode

Some vendor software might not be capable of communicating with the CIM agent in a secure fashion. You can still use this vendor software by configuring the CIM agent to run with only basic user and password security. Perform the following steps to configure the CIM agent to run in unsecure mode:

1. Using the Windows Start Menu facility, stop the CIMOM by selecting **Start → Programs →CIM agent for IBM DS Open API→Stop CIMOM service**.

2. Using the Windows Services facility, stop and start the Service Location Protocol (SLP) service by selecting **Start→ Settings→Control Panel**. Double-click **Administrative Tools** and double click **Services**. In the Name column, right-click **Service Location Protocol** and select **Stop**. After the SLP stops, start it again by right-clicking the **Service Location Protocol** again and select **Start**. After the SLP starts, close the Services Window and the Administrative Tools Window.

3. Find the cimom.properties file and edit it with a tool such as Notepad, setting the properties as shown in the following example:

   ```
   Port=5989 ServerCommunication=HTTP DigestAuthentication=False
   ```

   Once the CIMOM starts, it accepts requests over HTTP using basic authentication.

   Note: To completely disable security checking, set "Authorization=False" in the cimom.properties file.

4. Using the Windows Start Menu facility, restart the CIMOM by selecting **Start→Programs→CIM agent for IBM DS Open API→Start CIMOM service**. The CIMOM registers itself with SLP using the revised attributes.

5. Close this window by pressing any key when you are prompted by the following display:

   ```
   The CIM Object Manager service is starting .....

   The CIM Object Manager service was started successfully

   Press any key to continue ...
   ```

Verifying the CIM Agent Connection on Windows

During this task, the CIM agent software connects to the storage unit that you identified in the configuration task.

If you are managing an ESS, perform the following steps to verify that the configuration file for the ESS CLI (CLI.CFG) is set correctly and that you have a connection. If you are not managing an ESS, skip to step 4 to verify that you have a connection.

1. Verify that you have network connectivity to the ESS from the system where the CIM agent is installed. To do this, perform the following steps:

    a. Open a command prompt window.

    b. Issue a **ping** command to the ESS; for example:

    ```
    ping 9.11.111.111
    ```

    where *9.11.111.111* is the ESS IP address

    c. Check that you can see reply statistics from the ESS IP address. The following is example output:

    ```
    Pinging 9.11.111.111 with 32 bytes of data:

    Reply from 9.11.111.111: bytes=32 time<10ms TTL=255

    Reply from 9.11.111.111: bytes=32 time<10ms TTL=255

    Reply from 9.11.111.111: bytes=32 time<10ms TTL=255

    Reply from 9.11.111.111: bytes=32 time<10ms TTL=255
    ```

If you see other messages that indicate that the request has timed out, see your Network Administrator for help on establishing network connectivity from the system where the CIM agent is installed.

2. Verify that the ESS CLI is operational and can connect to the storage unit. To do this, perform the following steps:

    a. Open a command prompt window.

    b. Issue the following command:

    ```
    esscli -u essuser -p esspass -s 9.11.111.111 list server
    ```

where:

- *9.11.111.111* represents the IP address of the Enterprise Storage Server.
- *essuser* represents the DS Storage Manager user name.
- *esspass* represents the DS Storage Manager password for the user name.

The following is an example of a successful response:

```
Thu Oct 09 11:22:28 PDT 2003 IBM ESSCLI 2.4.0.236

Server Mode Mfg WWN CodeEC Cache NVS Racks

---------- ----- --- ---------------- --------- ----- --
--- -----

2105.22232 800 013 5005076300C09470 2.4.0.236 8GB 2GB
```

c. Verify that the CLI.CFG file is set correctly. From the command prompt window, issue the following command:

```
rsTestConnection.exe /s /v primaryservername
```

where

- */s primaryservername* represents the IP address or the complete host name of an ESS Copy Services server.
- */v* designates that all responses from the server be displayed.

Note: In some cases the ESS CLI does not work correctly unless the system has been rebooted following the new installation of the ESS CLI.

3. Using the Windows Services Facility, verify that the SLP is active by selecting **Start → Settings → Control Panel**. Double-click the **Administrative Tools** icon, and then double-click the **Services** icon.

   a. Find the Service Location Protocol (SLP) in the Name column. For this component, the Status column should be marked **Started** and the Startup Type column should be marked **Manual**. If either of those conditions are not met, right click on **Service Location Protocol** and click **Start** from the pop-up menu. Wait for the Status to change to **Started**.

   b. Do not close the Services window, because you will use it in the next step to verify that the CIMOM is started.

4. Verify that the CIMOM is active by finding **CIM Object Manager - DS Open API** in the Name column of the Services window. For this component, if the Status column is not marked **Started**, right click on **CIM Object Manager - DS Open API** and click **Start** from the pop-up menu. Wait for the Status to change to **Started**.

5. Verify CIMOM registration with SLP by selecting **Start → Programs → CIM agent for IBM DS Open API → Check CIMOM Registration**. The window closes when you press any key, as instructed in the output:

```
service: wbem:http://tpc035/ 5989, 65535

press any key to continue...
```

Note: If the verification of the CIMOM registration is not successful, stop and restart the SLP and CIMOM services.

6. Use the **verifyconfig** command to locate all WBEM services in the local network. This command verifies that you have configured the CIM agent and can connect to at least one ESS. Type the **verifyconfig** command in a command prompt window in the directory where the CIM agent was installed; for example:

```
c:\program files\ibm\cimagent>verifyconfig -u <username> -p
 <password>
```

where *username* is the user name and *password* is the password for the user name that you configured to manage the CIMOM.

If the command is successful, output similar to the following is displayed:

```
C:\program files\ibm\cimagent>verifyconfig -u guest -p
 guest

Verifying configuration of CIM agent for the IBM
 TotalStorage DS Open Application Programming Interface...

Communicating with SLP to find WBEM services...

3 WBEM services found

host=9.11.111.111, port=5989

host=9.11.111.112, port=5989

host=9.11.111.113, port=5989

Connecting to CIM agent, host=9.11.111.112, port=5989

Found 2 IBMTSESS_StorageSystem instances:
```

```
2107.AZ123x

2105.2223x

Internal Server at 9.11.111.122 configured for 2107.AZ123x

Internal Server at 9.11.111.119 configured for 2105.2223x

Verification Successful
```

Error Messages

You might encounter the following error messages:

Error Type 1. E CMMOM0002E CIM_ERR_ACCESS_DENIED

If you enter CIMOM user name or password that is not valid or forget to type the CIMOM user name or password when you issue the verifyconfig command, the following message series is displayed near the end of the output messages:

```
E CMMOM0002E CIM_ERR_ACCESS_DENIED

    at com.ibm.http.HTTPClient.sendRequest(Unknown Source)

    at com.ibm.http.HTTPClient.sendRequest(Unknown Source)

    at com.ibm.xml.XMLOperationGeneric.intrinsicMethod(Unknown
Source)

    at com.ibm.xml.XMLOperationGeneric.intrinsicMethod(Unknown
Source)

    at com.ibm.xml.XMLEnumerateInstances.enumInstances(Unknown
Source)

    at com.ibm.xml.CIMOMHandleXML.enumInstances(Unknown Source)

    at com.ibm.cim.CIMClient.enumInstances(Unknown Source)

    at com.ibm.cimom.install.VerifyConfig.enumInstances(Unknown
Source)

    at com.ibm.cimom.install.VerifyConfig.enumInstances(Unknown
Source)

    at com.ibm.cimom.install.VerifyConfig.main(Unknown Source)

 FAILED requesting IBMTSESS_StorageSystem instances
```

Error Type 2. CIM agent not correctly configured If any of the following are true:

- You have never used the setdevice tool to define a storage unit to the CIMOM.
- You made an error in the IP address, user name, or password.
- You did not restart the CIMOM after adding the ESS/DS.

The following message series is displayed near the end of the output messages:

```
Connecting to CIM agent, host=1.11.111.111, port=5989

Found 0 IBMTSESS_StorageSystem instances

CIM agent not correctly configured
```

You can find more information about the possible cause of this error message by examining the cimom*x*.log (where *x* can be a number from 1–9. For example, *cimom7.log*).

If you have a network connection problem or you have set an incorrect IP address for the ESS using the setdevice tool, the ESS CLI cannot connect to the ESS. A message pair similar to the following can appear in the log:

```
2003-10-30 08:37:03,PST-08:00
CIMOM[com.ibm.provider.ess.EssCLICmdHandler.
outputEssCliError(Unknown Source)]: ESSCLI Error
[java.lang.Object{esscli 204: The connection to the specified
server was not established.}]

2003-10-30 08:37:03,PST-08:00 E
CIMOM[com.ibm.provider.ess.EssProvider.initialize (Unknown
Source)]: esscli list server failed for 9.11.111.112, trying
again... [java.lang.Object{Operation Failed. RC=2}]
```

If you have entered an incorrect user name or password for the ESS using the **setdevice** tool, the ESS CLI can connect to the ESS but cannot *authenticate. A message pair similar to the following can appear in the log:*

```
2003-10-30 10:32:53,PST-08:00 E
CIMOM[com.ibm.provider.ess.EssCLICmdHandler.
outputEssCliError(Unknown Source)]: ESSCLI Error
[java.lang.Object{esscli 510: Access was denied by the server.}]

2003-10-30 10:32:53,PST-08:00 E
CIMOM[com.ibm.provider.ess.EssProvider.initialize (Unknown
Source)]: esscli list server failed for 9.11.111.112, trying
again... [java.lang.Object{Operation Failed. RC=5}]
```

If you did not reboot after you installed the ESS CLI or before you ran the CIM agent **verifyconfig** program, the ESS CLI will have a problem finding an environmental variable. A message similar to the following can appear in the log:

```
2003-10-29 17:26:02.608-08:00 [java.lang.Object{esscli: No value
is specified for the <INSTALL> system variable.}] I
CIMOM[com.ibm.provider.ess.EssProvider.initialize(Unknown
Source)]: store01.storage.sanjose.ibm.com IP esscli list server
failed, trying again...
```

Error Type 3. E CMMOM0001E CIM_ERR_FAILED(E CMMOM0001E CIM_ERR_FAILED)

If you have not installed the ESS CLI on your system, the following message series is displayed near the end of the output messages:

```
Connecting to CIM agent, host=1.11.111.11, port=5989 E CMMOM0001E
CIM_ERR_FAILED(E CMMOM0001E CIM_ERR_FAILED) at
com.ibm.xml.XMLOperationGeneric.processReturnStream(Unknown
Source) at com.ibm.xml.XMLOperationGeneric.intrinsicMethod(Unknown
Source)

at com.ibm.xml.XMLOperationGeneric.intrinsicMethod(Unknown Source)

at com.ibm.xml.XMLEnumerateInstances.enumInstances(Unknown Source)

at com.ibm.xml.CIMOMHandleXML.enumInstances(Unknown Source)

at com.ibm.cim.CIMClient.enumInstances(Unknown Source)

at com.ibm.cimom.install.VerifyConfig.enumInstances(Unknown
Source)

at com.ibm.cimom.install.VerifyConfig.enumInstances(Unknown
Source)

at com.ibm.cimom.install.VerifyConfig.main(Unknown Source)

FAILED requesting IBMTSESS_StorageSystem instances
```

Error Type 4. No CIM agent running or registered with SLP on current host

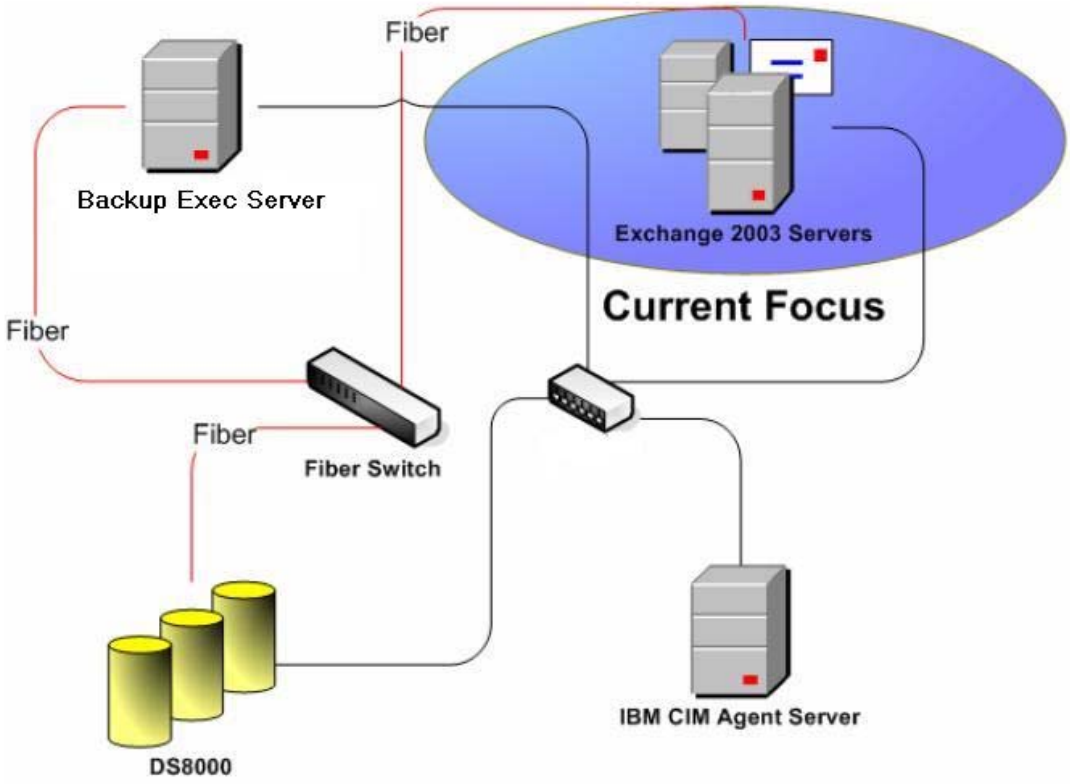
If the CIM agent is not started or it has not registered with SLP on the current host, the following message is displayed in the output messages in the Command Prompt window:

```
No CIM agent running or registered with SLP on current host
```

This completes the verification of the connection to the ESS/DS.

DS Open API Support for Microsoft Volume Shadow Copy and Virtual Disk Services for Windows

This chapter includes an overview of DS Open API support for Microsoft Volume Shadow Copy and Virtual Disk Services along with an overview of the installation process and instructions for installing and reconfiguring Microsoft Volume Shadow Copy and Virtual Disk Services on a Windows Server 2003 operating system. Instructions for uninstalling Microsoft Volume Shadow Copy and Virtual Disk Services are also provided.



DS Open API Support for Microsoft VSS and VDS Overview

The following information provides an overview of Microsoft Volume Shadow Copy Service and Virtual Disk Service.

Microsoft Volume Shadow Copy Service

DS Open API Support for Microsoft Volume Shadow Copy and Virtual Disk Services controls storage units using a CIM client query.

You must install the CIM agent, a middleware application that provides a CIM-compliant interface, before installing Microsoft Volume Shadow Copy and Virtual Disk Services. The Microsoft Volume Shadow Copy and Virtual Disk Services use the CIM technology to manage proprietary devices as open system devices through storage management applications.

DS Open API support for Microsoft Volume Shadow Copy Service enables users to quickly backup and restore large amounts of data on Windows Server 2003. Microsoft Volume Shadow Copy Service coordinates with a provider and the storage unit to create a consistent shadow copy of a volume or group of volumes at a point-in-time. Point-in-time shadow copies ensure consistency for Microsoft Volume Shadow Copy Service-aware writers, and also work with applications that do not support Microsoft Volume Shadow Copy Service technology. The shadow copy can be created while the volume is mounted and files are in use.

In order to accomplish this fast backup, a backup application initiates a shadow copy backup. Microsoft Volume Shadow Copy Service then coordinates with the Microsoft Volume Shadow Copy Service writers to briefly quiesce writes to the databases, applications, or both. Next, Microsoft Volume Shadow Copy Service flushes the file system buffers and asks a provider to initiate a FlashCopy of the data. Once the FlashCopy is logically complete, Microsoft Volume Shadow Copy Service allows application writes to resume.

The volumes are then mounted hidden and read-only, to be used when rapid restore is necessary. Alternatively, the volumes can be mounted on a different host and used for application testing or backup to tape.

Microsoft Virtual Disk Service

DS Open API Support for Microsoft Virtual Disk Service provides a single vendor and technology neutral interface designed to manage block storage virtualization, whether done by OS software, RAID storage hardware, or other storage virtualization engines. Microsoft Virtual Disk Service is designed to enable the management of heterogeneous storage systems, by using both client and provider APIs. The service is designed to allow you to perform the following functions:

- List Information about:
    - Providers
    - Subsystems
    - Controllers
    - LUNs
    - Drives
- Create or delete LUNs

- Configure LUNs automatically, which facilitates dynamic reconfiguration by hardware in response to load or fault handling.

DS Open API Support for Microsoft VSS and VDS Installation Overview

This section provides an overview of the installation and configuration of Microsoft Volume Shadow Copy and Virtual Disk Services on a Windows Server 2003 operating system. You should have knowledge of how to administer a Windows Server 2003 operating system before you install Microsoft Volume Shadow Copy Service or Virtual Disk Service. You should also become familiar with the installation tasks and gather all of the information you will need for installation ahead of time.

The following installation tasks are presented in the order that they must be performed:

1. Before you install Microsoft Volume Shadow Copy or Virtual Disk Services, check the hardware and software requirements.
2. Install the prerequisite CIM agent software.
3. Run the InstallShield Wizard for Microsoft Volume Shadow Copy and Virtual Disk Services to install the CIM agent.
4. Verify the installation.
5. Create free and reserved volume pools.
6. Reconfigure the services. Perform this optional task if you would like to change the configuration that you established during installation.

DS Open API Support for Microsoft VSS and VDS Installation Requirements

Ensure that your system satisfies the following prerequisite for installing Microsoft Volume Shadow Copy and Virtual Disk Services on a Windows Server 2003 operating system before you start the installation.

You must install the CIM agent *before* you install the Microsoft Volume Shadow Copy and Virtual Disk Services. You can install the CIM agent on the same machine as Microsoft Volume Shadow Copy and Virtual Disk Services or on a different machine.

Hardware Requirements

The following minimum hardware is required:

- For Volume Shadow Copy Services & Virtual Disk Services: a DS8000, DS6000, or ESS storage unit (with FlashCopy Version 1 or 2)
- A system capable of running Windows Server 2003
- 133 – 733+ megahertz CPU
- 128 – 256+ megabytes of random access memory
- 1.5+ gigabytes of disk space
- Supported QLogic or Emulex Fibre Channel host bus adapter (HBA)

Software Requirements

The following software is required:

- Windows Server 2003 Service Pack 2 operating system. The following editions of Windows Server 2003 are supported:
    - Enterprise Edition, 32-bit version
    - Datacenter Edition, 32-bit version
- Common Information Model (CIM) agent. The CIM agent can be installed on the same machine as Microsoft Volume Shadow Copy Service or on a different machine. You can find this software on the CIM agent for IBM TotalStorage DS Open Application Programming Interface CD.
- Microsoft Volume Shadow Copy Service compliant backup software

Installing the DS Open API Support for Microsoft VSS and VDS on Windows

This section includes the steps to install the DS Open API support for both Microsoft Volume Shadow Copy and Virtual Disk Services on your Windows system.

You must satisfy all prerequisites that are listed in the installation requirements section before you start the installation.

1. Log on to your system as the local administrator.
2. Run the InstallShield Wizard by inserting the *IBM DS Open Application Programming Interface support for Microsoft Volume Shadow Copy and Disk Services CD* into the CD-ROM drive.
3. The **Welcome** window opens. Click **Next** to continue with the InstallShield Wizard. You can click **Cancel** at any time exit the installation, or click **Back** to move back to previous screens.

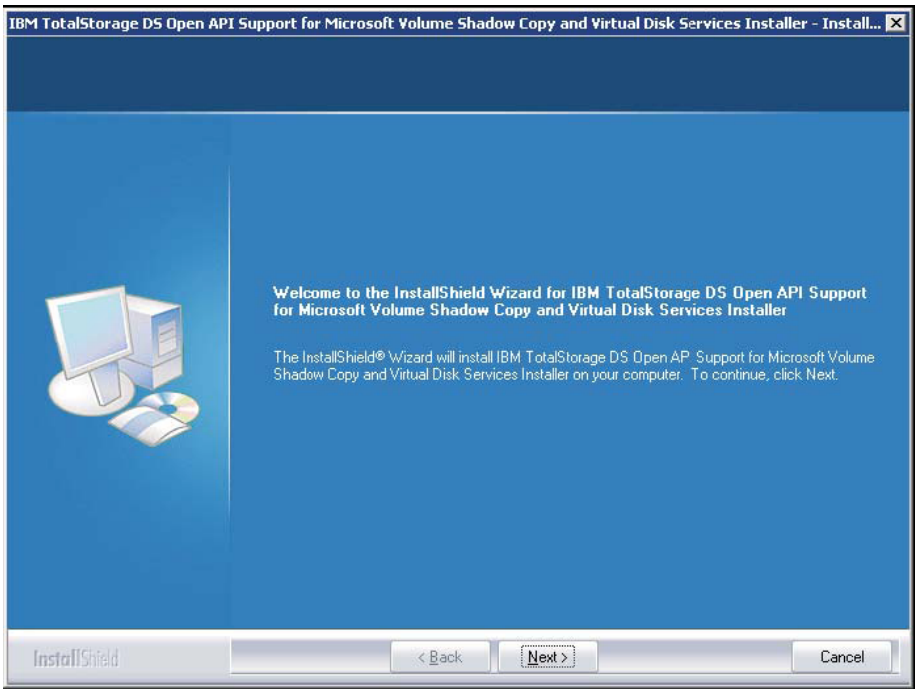


Figure 7: Installation Wizard for Microsoft Volume Shadow Copy and Virtual Disk Services

4. Read and accept the license agreement, and then click **Next** to continue. If you do not accept, you cannot continue with the installation.

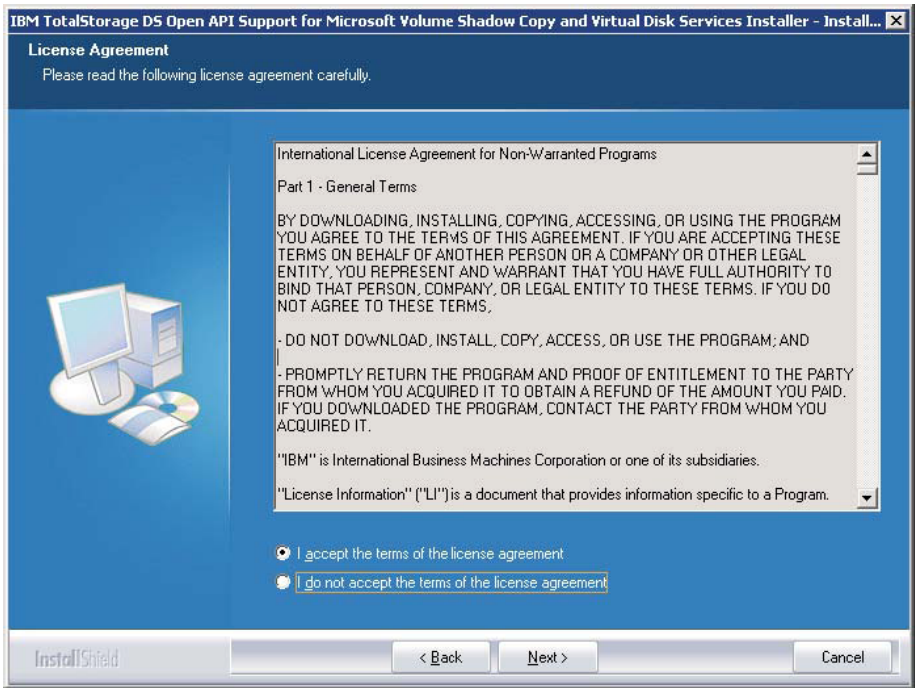


Figure 8: License Agreement

5. The **Edit Data** window opens. In order to connect to the CIM agent, Microsoft Volume Shadow Copy and Disk Services must obtain some information about the server that the CIM agent is installed on. Type the required CIM agent port, host, and user information, and then click **Next**.

   Note:

   - If these settings change after installation, you can use the *ibmvcfg.exe* tool to update Microsoft Volume Shadow Copy and Virtual Disk Services with the new settings.

   - If you do not have the CIM agent port, host, or user information, contact your CIM agent administrator.

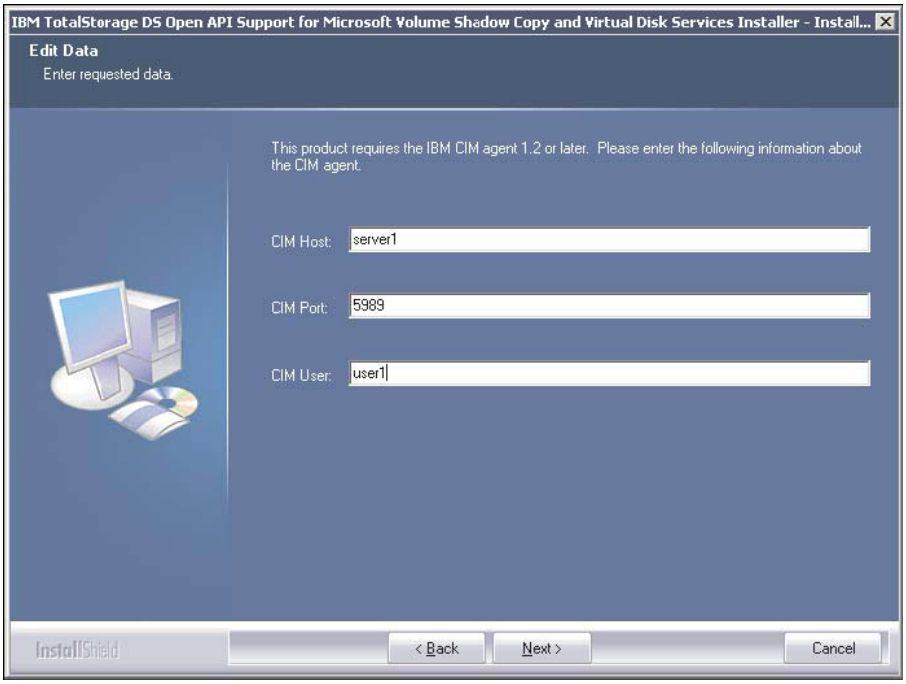


Figure 9: The Edit Data window

6. The **Password** window opens. Enter your CIM agent password and click **Next**.

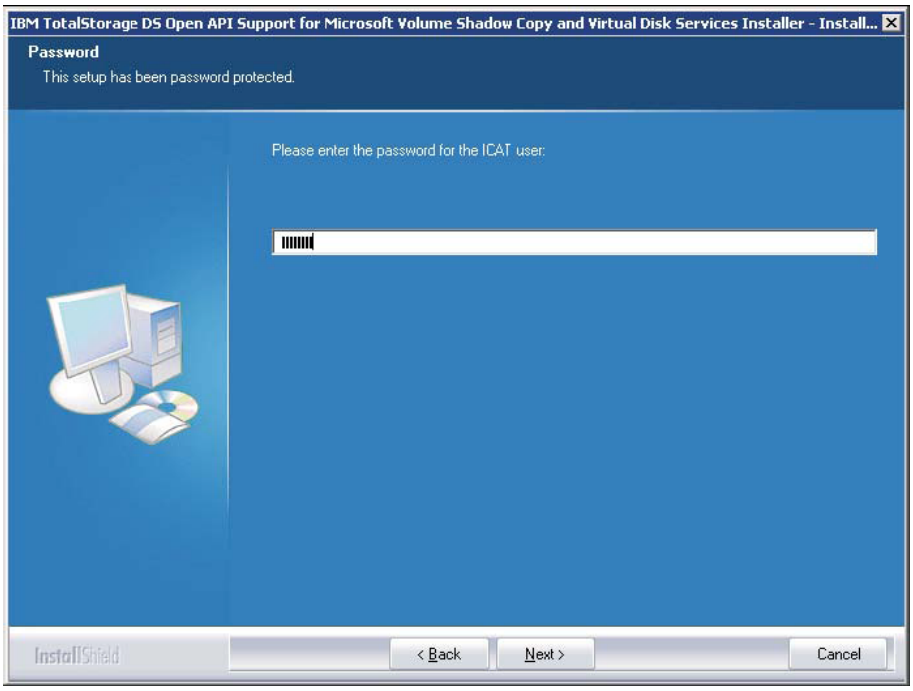


Figure 10: The Password window

7. The **Setup Type** window opens. Select whether you want to use Secure Sockets Layer (SSL) to connect to the CIM agent and click **Next**.

   Note:

   - You can set the SSL using the *ibmvcfg.exe* configuration tool.
   - If you are not sure whether to use SSL to connect to the CIM agent, contact your CIM agent administrator.

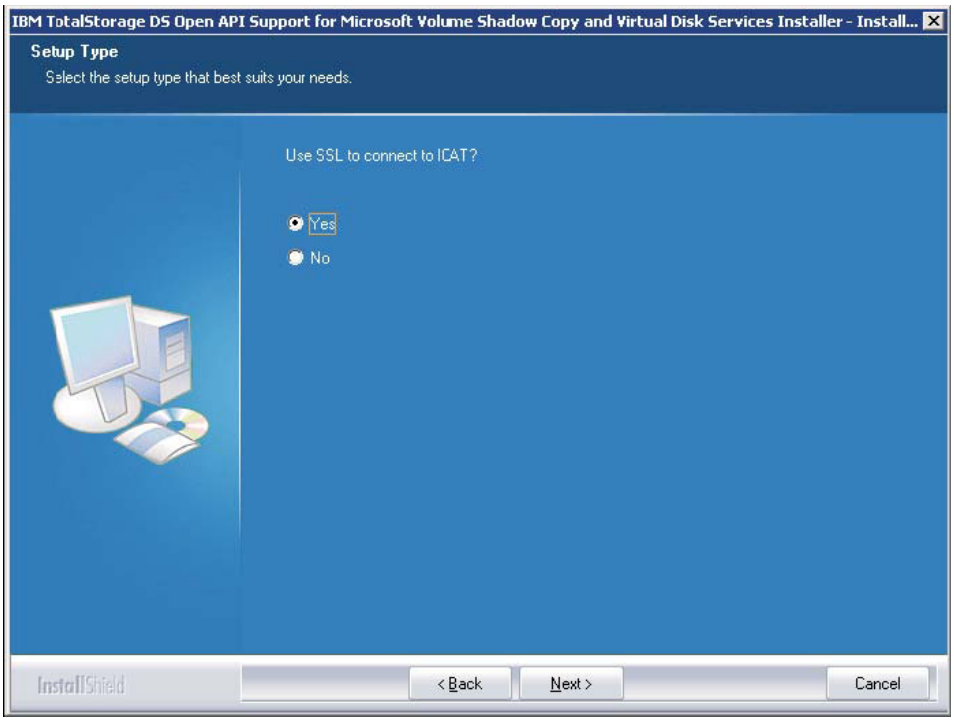


Figure 11: Setup Type window

8. The **Edit Data** window opens. Type the location of the CIM agent truststore file. This truststore file is generated during the CIM agent installation. You must copy this file to a location accessible by Microsoft Volume Shadow Copy and Virtual Disk Services. Then type the truststore password and click **Next**.

   Note: The default CIM agent truststore password is “ibmstore”. If the CIM agent truststore password has been changed from the default and you do not have this information, contact your CIM agent administrator. You can change the CIM agent truststore password using the *ibmvcfg.exe* configuration tool.

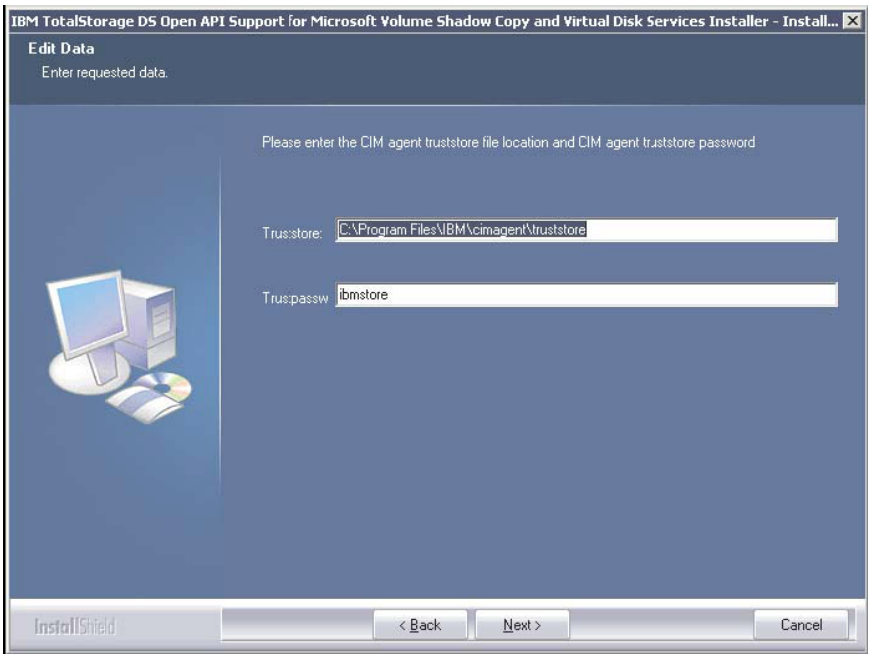


Figure 12: Edit Data window

9. The **Choose Destination Location** window opens. Click **Next** to accept the default directory where the setup will install the files, or click **Change** to select a different directory and then click **Next**.

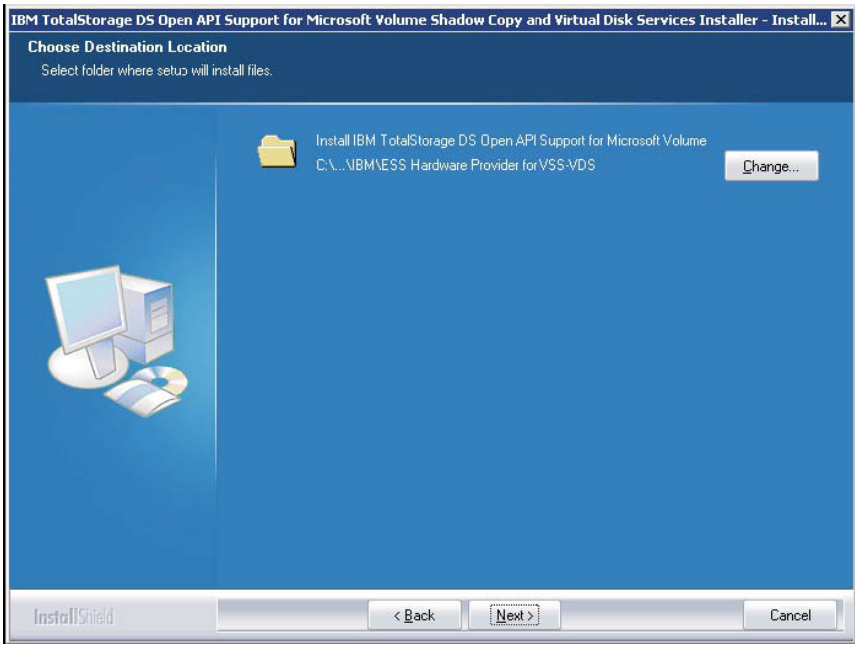


Figure 13: Choose Destination Location window

10. The **Ready to Install the Program** window opens. Click **Install** to begin the installation.

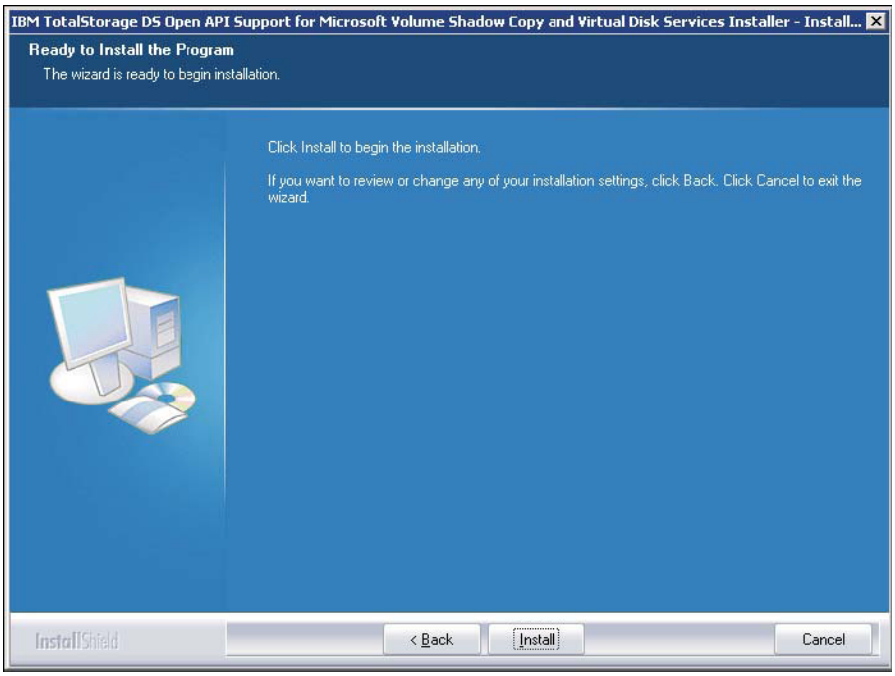


Figure 14: Ready to Install the Program window

The **Setup Status window** displays the progress of the installation. Wait for the setup to complete, or click **Cancel** if you want to abort the setup.

11. The **InstallShield Wizard Complete** window opens when the installation has finished. Click **Finish** to exit the wizard.

12. The installation program might prompt you to reboot your system.

If you are able to perform all of the installation tasks successfully, then the Microsoft Volume Shadow Copy Service has been successfully installed on your Windows system.

Verifying the DS Open API Support for Microsoft VSS and VDS Windows Installation

This task verifies that the services that you selected to install are correctly installed on your system. During installation, you had the option to install Microsoft Volume Shadow Copy Service, Microsoft Virtual Disk Service, or both.

Perform the following steps to verify the installation of the services that you selected to install:

1. If verifying Microsoft Volume Shadow Copy Service installation, select **Start → All Programs → Administrative Tools → Services**

2. Ensure that there is a service named IBM DS Open API Support for Microsoft Volume Shadow Copy that is listed, and that the Status is Started and the Startup Type is Automatic.

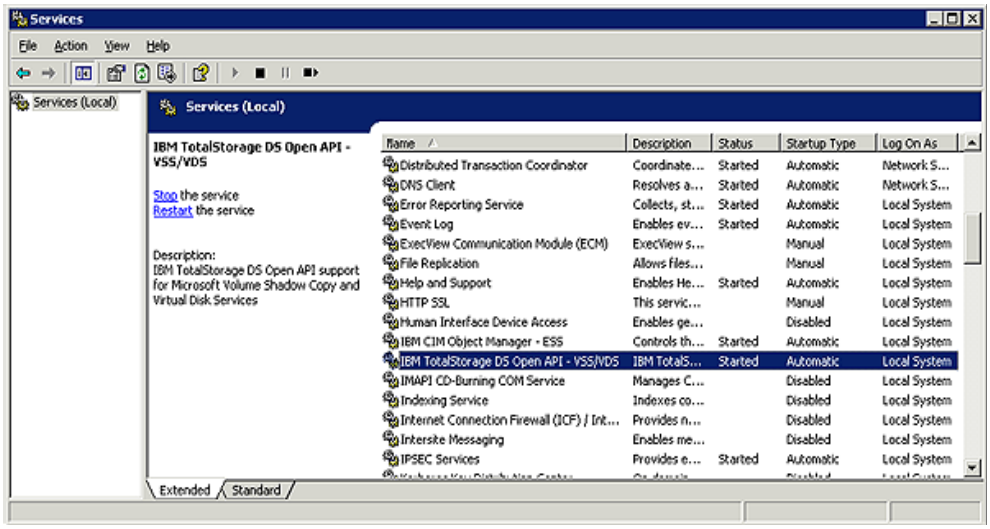


Figure 15: Service verification

3. Open a command prompt window and type the following command to verify that DS Open API Support for Microsoft Volume Shadow Copy and Virtual Disk Services are installed:

```
vssadmin list providers

Ensure each service that you installed is listed as a provider.
```

If you are able to perform all of these verification tasks successfully, either Microsoft Volume Shadow Copy, Virtual Disk Services, or both, have been successfully installed on your Windows system.

Creating VSS_FREE and VSS_RESERVED Pools for Microsoft VSS

This task allows you to create the VSS_FREE and VSS_RESERVED pools.

Before using the IBM DS Open API support for Microsoft Volume Shadow Copy for the first time, you must designate which volumes that the services can use as FlashCopy target volumes. This designation is done by creating a VSS_FREE pool and a VSS_RESERVED pool, represented by virtual hosts that are created on the storage unit. Once the virtual hosts are created, volumes can be added to the free pool by simply assigning a volume to the virtual host.

Perform the following steps using the IBM DS Storage Manager or DSCLI to create the VSS_FREE and VSS_RESERVED pools:

Note: If you are using the DSCLI you must perform these steps in order.

1. Create a volume group with the name ″VSS_FREE″ or another name, of the same type as your Windows Server 2003 host, for example: SCSI Map 256.
2. Create a virtual hostconnect on the storage unit named ″VSS_FREE″ or another name, with the following parameters:
    a. -profile ″Intel - Windows 2003″
    b. -addrdiscovery LUNPolling
    c. -*volgrp* Where *volgrp* is volume group created in step 1.
    d. -wwname 5000000000000000
3. Create a volume group with the name ″VSS_RESERVED″ or another name, of the same type as your Windows Server 2003 host, e.g. SCSI Map 256.
4. Create a virtual hostconnect on the storage unit named ″VSS_RESERVED″ or another name, with the following parameters:
    a. -profile ″Intel - Windows 2003″
    b. -addrdiscovery LUNPolling
    c. -*volgrp* Where *volgrp* is volume group created in step 3.
    d. -wwname 5000000000000001
5. Create and assign free volumes to the VSS_FREE volume group.

    Note: If you already have volumes that are created for the VSS_FREE virtual host, you must assign those volumes to VSS_FREE.

Verifying DS Open API Support for Microsoft VSS and VDS Windows Configuration

This task verifies that Microsoft Volume Shadow Copy and Virtual Disk Services are configured correctly on your Windows system.

After you have created the VSS_FREE and VSS_RESERVED pools for Microsoft Volume Shadow Copy Service, perform the following steps to verify your configuration:

1. Issue the following command:

   ```
   ibmvcfg listvols
   ```

   All of the volumes on your storage unit are listed with the worldwide port names (WWPNs) that they are assigned to.

2. If the volumes are not listed, check the connectivity of your CIM agent. Then, check your DS Open API support for Microsoft Volume Shadow Copy and Virtual Disk Services configuration. You can reconfigure using the commands that are listed in the next section. The IBMVSS.log provides more detailed information on which of the settings is incorrect. DS Open API support for Microsoft Volume Shadow Copy and Virtual Disk Services do not work if this command does not complete successfully.

Result:

If you are able to perform all of the verification tasks successfully, Microsoft Volume Shadow Copy and Virtual Disk Services have been successfully configured on your Windows system.

DS Open API Support for Microsoft VSS and VDS Reconfiguration Commands

After installation, you can use several commands on the ibmvcfg.exe tool to change or correct parameters that you used to install the Microsoft Volume Shadow Copy and Virtual Disk Services. To do this, you must use the utility ibmvcfg.exe. You do not have to set many of the settings because there are defaults that are provided for them in Microsoft Volume Shadow Copy and Virtual Disk Services. The following table shows the commands that you can use for reconfiguration.

Note: If you do not know which settings to provide (for example, passwords or user names) for the following commands, contact your system administrator.

Command	Description	Example
ibmvcfg showcfg	Provides the current settings.	
	CIMOM settings	
ibmvcfg set username <CIMOM username>	Sets the CIMOM user name.	ibmvcfg set username johnny

ibmvcfg set password <CIMOM password>	Sets the CIMOM user password.	ibmvcfg set password mypassword
ibmvcfg set trustpassword <trustpassword>	Sets the CIMOM trust password.	ibmvcfg set trustpassword trustme
ibmvcfg set truststore <truststore location>	Specifies the truststore file location.	ibmvcfg set truststore c:\truststore
ibmvcfg set usingSSL	Specifies whether to use Secure Socket Layers to connect to the CIMOM.	ibmvcfg set usingSSL yes
ibmvcfg set cimomPort <portnum>	Specifies the CIMOM port number. The default value is 5989.	ibmvcfg set cimomPort 5989
ibmvcfg set cimomHost <server name>	Sets the name of the CIMOM server.	ibmvcfg set cimomHost cimomserver
ibmvcfg set namespace <namespace>	Specifies the namespace value that CIMOM is using. The default value is \root\ibm.	ibmvcfg set namespace \root\ibm
	Volume Shadow Copy Service settings	
ibmvcfg listvols	Lists the volumes that are currently in the freepool, unassigned, or all volumes. By default, without any additional parameters, this command lists all of the volumes.	ibmvcfg listvols ibmvcfg listvols free ibmvcfg listvols unassigned ibmvcfg listvols all
ibmvcfg listvols free	Lists the volumes that are currently in the freepool, unassigned, or both.	ibmvcfg listvols free
ibmvcfg listvols unassigned	Lists the volumes that are currently in the freepool, unassigned, or both.	ibmvcfg listvols unassigned
ibmvcfg add	Adds a volume or volumes to the freepool.	ibmvcfg add 12312345 32112345
ibmvcfg rem	Removes a volume or volumes from the freepool.	ibmvcfg rem 512 ibmvcfg rem 51212345

ibmvcfg set vssFreeInitiator <WWPN>	Specifies the WWPN that designates the freepool. The default value is 5000000000000000. Modify this value only if there is a host already in your environment with a WWPN of 5000000000000000.	ibmvcfg set vssFreeInitiator 5000000000000000
ibmvcfg set vssReservedInitiator <WWPN>	Specifies the WWPN that designates the reservedpool. The default value is 5000000000000001. Modify this value only if there is a host already in your environment with a WWPN of 5000000000000001.	ibmvcfg set vssFreeInitiator 5000000000000001
ibmvcfg set FlashCopyVer <1 | 2>	Sets the FlashCopy version that is available on the storage unit. The default value is 1.	ibmvcfg set FlashCopyVer
	Virtual Disk Service settings	
None		

Error Codes Returned by Microsoft VSS and VDS

The following table lists Microsoft Volume Shadow Copy and Virtual Disk Services error codes.

Note: These errors are logged in the Windows Event Monitor and in the Microsoft Volume Shadow Copy and Virtual Disk Services log file that is located in the directory chosen during installation.

Symbolic Name	Code	Definition
ERR_JVM	1000	JVM Creation failed.
ERR_CLASS_NOT_FOUND	1001	Class not found: %1.
ERR_MISSING_PARAMS	1002	Some required parameters are missing.
ERR_METHOD_NOT_FOUND	1003	Method not found: %1.
ERR_REQUIRED_PARAM	1004	A missing parameter is required. Use the configuration utility to set this parameter: %1.
ERR_RECOVERY_FILE_CREATION_FAILED	1600	The recovery file was not created.

ERR_ARELUNSSUPPORTED_IBMGETLUNINFO	1700	ibmGetLunInfo failed in AreLunsSupported.
ERR_FILLLUNINFO_IBMGETLUNINFO	1800	ibmGetLunInfo failed in FillLunInfo.
ERR_GET_TGT_CLEANUP	1900	Failed to delete the following temp files: %1
ERR_LOG_SETUP	2500	Error initializing log.
ERR_CLEANUP_LOCATE	2501	Unable to search for incomplete Shadow Copies. Windows Error: %1.
ERR_CLEANUP_READ	2502	Unable to read incomplete Shadow Copy Set information from file: %1.
ERR_CLEANUP_SNAPSHOT	2503	Unable to cleanup snapshot stored in file: %1.
ERR_CLEANUP_FAILED	2504	Cleanup call failed with error: %1.
ERR_CLEANUP_OPEN	2505	Unable to open file: %1.
ERR_CLEANUP_CREATE	2506	Unable to create file: %1.
ERR_HBAAPI_LOAD	2507	HBA: Error loading HBA library: %1.
ERR_ESSSERVICE_EXCEPTION	3000	ESSService: An exception occurred. Check the ESSService log.
ERR_ESSSERVICE_LOGGING	3001	ESSService: Unable to initialize logging.
ERR_ESSSERVICE_CONNECT	3002	ESSService: Unable to connect to the CIM agent. Check your configuration.
ERR_ESSSERVICE_SCS	3003	ESSService: Unable to get the Storage Configuration Service. Check your configuration.
ERR_ESSSERVICE_INTERNAL	3004	ESSService: An internal error occurred with the following information: %1.

ERR_ESSSERVICE_FREE_CONTROLLER	3005	ESSService: Unable to find the VSS_FREE controller.
ERR_ESSSERVICE_RESERVED_CONTROLLER	3006	ESSService: Unable to find the VSS_RESERVED controller. Check your configuration.
ERR_ESSSERVICE_INSUFFICIENT_TARGETS	3007	Unable to find suitable targets for all volumes.
ERR_ESSSERVICE_ASSIGN_FAILED	3008	ESSService: The assign operation failed. Check the CIM agent log for details.
ERR_ESSSERVICE_WITHDRAW_FAILED	3009	ESSService: The withdraw FlashCopy operation failed. Check the CIM agent

Validate VSS Operations with Vshadow.exe

Before installing backup applications, it is highly recommended that core VSS functionality be tested. VSS functionality can be validated with the VSHADOW tool, which is a lightweight VSS requestor available from Microsoft. The following are the VSHADOW tests recommended before any backup software is installed.

1. Test Non-persistent shadow copy creation and deletion.

   At a command prompt, type:

   ```
   VSHADOW k: l:
   ```

   Note: k: and l: represent the Exchange Database and log volumes.

   Repeat this 4 times. Verify the Windows Event Log contains no errors.

2. Test Persistent shadow copy creation and deletion.

   At a command prompt, type:

   ```
   VSHADOW -p k: l:
   ```

   You may need to run the following if there are space limitations:

   ```
   VSHADOW –da
   ```
   (Deletes all local shadow copies)

   Repeat this 4 times. Verify the Windows Event Log contains no errors.

3. Test Non-persistent transportable shadow copy creation and deletion

   At a command prompt type:

   ```
   VSHADOW -t=export.xml k: l:
   ```

   With VSHADOW, you must manually copy the .xml file to the offload server.

   On the machine you have set aside for offload, type:

   ```
   VSHADOW -i=export.xml
   ```

   Verify the Windows Event Log contains no errors.

After all of these tests complete without errors, you are ready for the Backup Exec component installation.

Installing Symantec Backup Exec for Windows Servers

This section contains excerpts from the **Backup Exec 11d For Windows Servers Administrators Guide.** For more detailed information, please consult the Administrators Guide.

Backup Exec Overview

Symantec Backup Exec for Windows Servers is a high-performance data management solution for Windows® server networks. With its client/server design, Backup Exec provides fast, reliable backup and restore capabilities for servers and workstations across the network. Backup Exec is available in configurations that can accommodate multi-platform networks of all sizes.

The Backup Exec suite includes agents and options for backing up and restoring data on many Microsoft operating systems and server products.

Backup Exec has supported Exchange since its introduction, delivering established experience and proven reliability in the Exchange Server market. In addition to support for VSS backup and restore, Backup Exec Agent for Microsoft Exchange Server introduces two key new technologies for Exchange to address the limitations of traditional Exchange backups:

- Granular Recovery Technology (GRT), including recovery from VSS snapshot backups.
- Continuous Data Protection for Exchange. While not the focus of this solution, CDP is another innovative Backup Exec technology that eliminates the need for daily backup windows. Continuous Data Protection does not currently support MSCS clusters or VSS.

These technologies eliminate not only separate individual mailbox backups but also time consuming and intrusive daily backups, along with Exchange protection management headaches. Symantec believes these technologies provide the fastest and most flexible way to protect and recover Exchange 2000 or 2003 Server data. For information on feature support for Exchange Server 2007, please visit the Symantec website:

http://www.symantec.com/smb/products/overview.jsp?pcid=bu_rec&pvid=bewin_svr

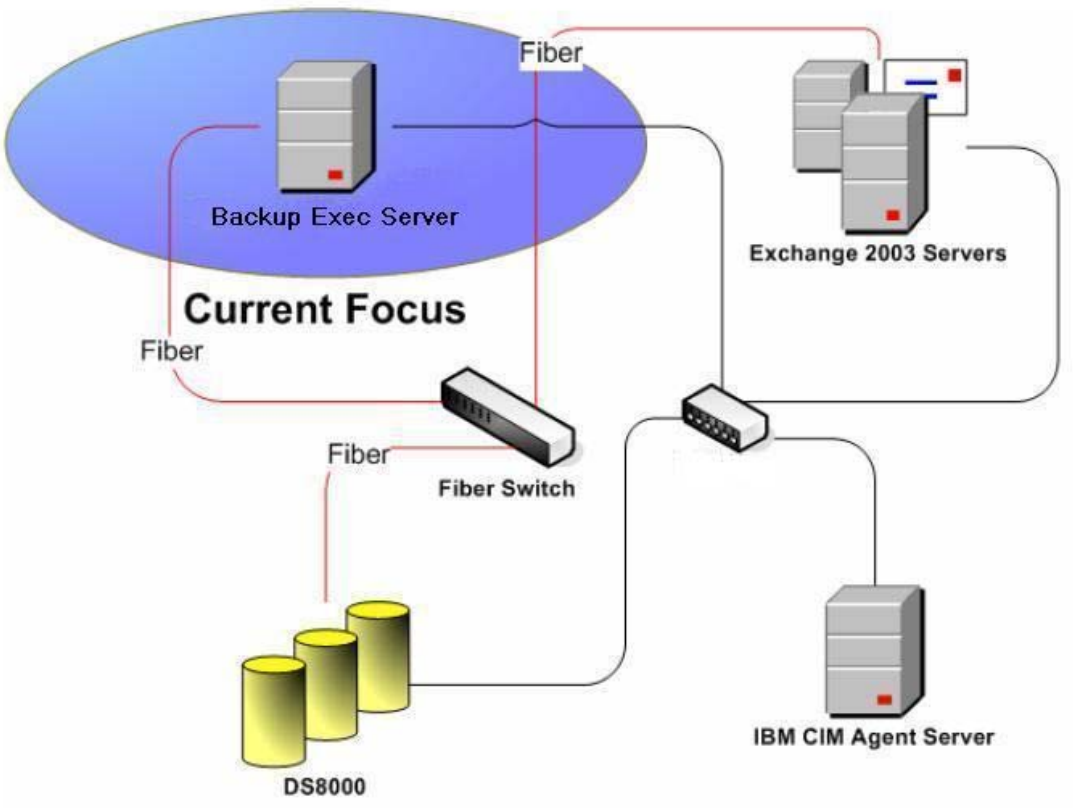
Backup Exec Installation Overview

This section provides system requirements, license key information, and step-by-step instructions for installing Backup Exec 11d for Windows Servers, Clients, and optional components.

For more detailed information about the following installation or configuration sections, please see the Symantec Backup Exec for Windows Servers Administrator's Guide. This guide is available on the installation CD or in online help format within Backup Exec. The Administrator's Guide provides complete instructions to help you set up and use Backup Exec.

Before you install Backup Exec, you should perform the following tasks:

- Run the Backup Exec Environment Check on the computer on which you want to install Backup Exec. The Environment Check analyzes the computer to make sure that the installation process can complete. If Backup Exec finds configuration issues that can be fixed during the installation, or that may prevent the installation, warnings appear. Although the Environment Check runs automatically during installation, you may want to run it manually before you install Backup Exec or before you back up data with Backup Exec.
- Install the storage device hardware (controller, drives, robotic libraries) on the media server. Refer to the documentation that is included with your storage device hardware for installation instructions. Use the appropriate Windows hardware setup functions to configure your controller and storage devices. Refer to your Microsoft Windows documentation for more information.
- Check your Windows security settings to make sure they work properly with the Backup Exec service account.
- If the drive on which you want to install Backup Exec is encrypted or compressed, and you would like to use a default SQL Express database, verify that an unencrypted and uncompressed drive is available for SQL Express installation.
- Exit all other programs.



Backup Exec Installation Requirements

Before installing your Backup Exec product, make sure you have the most current operating system patches and updates applied to your system. If you are not certain of your operating system level, contact your operating system vendor and request the latest patches and upgrades.

The following are the minimum system requirements for running version 11d of BackupExec:

Operating system

- Microsoft Windows 2000 Server (with Service Pack 4 and Update Rollup 1 for Service Pack 4)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Editions
- Microsoft Windows Server 2003 R2 Editions
- Microsoft Windows Storage Server 2005
- Microsoft Windows XP (with Service Pack 2)
- Microsoft Windows XP Professional x64 Edition

- Microsoft Windows Small Business Server 2000 (with Service Pack 4)
- Microsoft Windows Small Business Server 2003 (with Service Pack 1)

Additional application support

- Microsoft Windows Microsoft Management (MOM) 2005
- Microsoft Windows Data Protection Manager
- Microsoft SQL Server 2003, 2005
- Microsoft Sharepoint Portal Server 2001, 2003

Internet browser

- Internet Explorer 6.0 or later.

Processor

- Intel Pentium, Xeon, AMD, or compatible.

Memory

- Required: 256 MB RAM
- Recommended: 512 MB RAM (or more for better performance)
- RAM requirements may vary depending on the operations performed, the options installed, and the specific computer configuration.
- For the Central Admin Server Option: 512 MB RAM required, 1 GB recommended.
- Virtual Memory Recommendations: 20 MB above the Windows recommended size for total paging file size (total for all disk volumes).

Disk space

- 696 MB (Typical installation)
- 805 MB (Includes all options)
- Disk space requirements may vary depending on the operations performed, the options installed, and the specific system configuration. Backup Exec databases and catalogs will require additional space.

Other hardware

- Network interface card or a virtual network adapter card.
- CD-ROM drive.

- (Recommended) A mouse.
- (Optional for pager notification) Modem supported by Microsoft Windows.
- (Optional for printer notification) Printer supported by Microsoft Windows.

Storage hardware

- Backup Exec requires at least one storage media drive or single-drive robotic library and the appropriate controller card.
- You can also use removable storage devices and non-removable hard drives. Refer to the Backup Exec hardware compatibility list for a complete list of supported devices:

  http://support.veritas.com/docs/282249.

The Backup Exec Service Account

All Backup Exec services on the media server run in the context of a user account configured for the Backup Exec system services. You can create this account prior to the Backup Exec installation, or you can use an existing user account. To create a service account for Backup Exec during installation, enter the name and password of an Administrator account for the Backup Exec services to use. A separate dedicated service account for Backup Exec is recommended.

Use a Domain Administrators account, or an equivalent account that is part of the Domain Admins group. The account should also be assigned Exchange Administrator rights, which are set within the Exchange System Manager.

The account that you designate for Backup Exec services, whether it is a new account or an existing user account, is assigned the following rights:

- Authenticate as any user and gain access to resources under any user identity.
- Create a token object, which can then be used to access any local resources.
- Log on as a service.
- Administrative rights (provides complete and unrestricted rights to the computer).
- Backup operator rights (provides rights to restore files and directories).
- Manage auditing and security log.

Due to security implementations in Microsoft Small Business Server, the service account must be Administrator.

Installing Backup Exec for Windows Servers

The Backup Exec CD includes an installation program that guides you through the installation process.

Note: If you install Backup Exec through Terminal Services and the installation media is on a shared drive (CD-ROM or network share), you must install it using a UNC path. Installation via mapped drives is not supported in this situation.

To install Backup Exec on the media server / local computer:

1. From the installation CD browser, click **Installation**, and then click **Start the Backup Exec Installation**. Select the option to install Symantec Backup Exec.
2. On the Welcome panel, click **Next**.
3. Select 'I accept the terms of the license agreement', and then click **Next**.
4. Check Local Install, and then click Install Backup Exec software and options.
5. Click **Next.** For first-time installations and for upgrades, the Backup Exec Environment Check runs automatically after you click **Next**.
6. Review the results of the Environment Check.
7. Do one of the following:
   - If the Environment Check does not reveal any issues that may prevent a successful installation of Backup Exec, click **Next**.
   - If the Environment Check reveals any issues that may prevent a successful installation of Backup Exec, click **Cancel** to exit the wizard. Correct the issues before you attempt to install again.
8. Do one of the following:

   If you have serial numbers for Backup Exec and its options:

   - Go to **https://licensing.symantec.com** to activate the product. After you activate the product, Symantec sends license keys to you. License keys are required to install Backup Exec and its options. You can access the Web site from any computer that has Internet access.

- When you receive your license keys, go to step 9

If you have license keys for Backup Exec and its options go to step 9.

9. Select one of the following methods to enter license keys:

   To manually enter license keys:

   a. Type a license key into the license key field.

   b. Click Add.

   c. Repeat for each license key for each option or agent that you want to add.

   To import license keys from a file:

   a. Click Import.

   b. Select the besernum.xml file.

   To install an evaluation version:

   a. Leave the license key field blank.

   b. Proceed to step 10.

10. Click **Next**. The license keys that you entered are saved to the besernum.xml file, located in the Windows or WINNT directory.

11. Select any additional features to install.

    For this solution, you must select the following optional components to enable VSS backup capabilities for Exchange:

    - Advanced Open File
    - Advanced Disk-based Backup
    - Exchange Agent

    All features that you do not select have a red X in the feature icon. To enable any of these options, click the X, and then click **This feature will be installed on <computer name's> hard drive**. If the feature icon is shaded, the option is not available for change.

12. Accept the default installation directory (recommended) or click Change to specify a different directory.

13. Click **Next**.

14. Provide the BackupExec system account user name, password, and domain. This must be a domain Administrator account. See the above section entitled “About the BackupExec service account” for details about this account.

15. On the Symantec Backup Exec Database panel, do one of the following to select a location to store the Backup Exec database:

    To create a local Backup Exec SQL Express instance:

    a. Click **Create a local Backup Exec SQL Express instance** to **store the database on**.

    b. To change the location of the database, click **Browse**.

    c. Select the location, and then click OK.

    To use an existing SQL Server 2000 or SQL Server 2005 instance:

    a. Click **Use an existing SQL Server 2000 (SP3a or later) or SQL Server 2005 Server instance on the network to store the database on**.

    b. Select the instance.

    Note: When Backup Exec is installed into an existing instance, the automated master database restore feature is not available. To recover the Master database, you must replace it with the Master database copy that Backup Exec automatically creates and updates when the Master database is backed up. When Backup Exec is installed into an existing instance, the Cluster Configuration Wizard is not available.

16. Click **Next,** Backup Exec connects to the Database.

17. If the Select path to SQL Express setup file panel appears, perform the following steps to identify the location of the SQL Express SP1 setup file:

    a. Click **Browse**.

    b. Navigate to the location where you downloaded the SQL Express SP1 setup file.

    c. Click **OK**.

    d. Click **Next**.

18. If prompted, select how the Symantec Device Driver Installer should install device drivers for the tape storage devices that are connected to the server, and then click **Next**. It is recommended that you select **Use Symantec device drivers for all tape devices**.

19. If you are prompted, enter information or choose settings for additional options that you want to install. Click **Next** after each selection.
20. Review the Backup Exec installation review, and then click **Install** to continue.
21. The installation process takes several minutes to complete. During the process, the progress bar may not move for several minutes.
22. When the installation is complete, you can view the readme, create a shortcut to Backup Exec on the desktop, and restart the computer.
23. Click **Finish** to close the installation wizard.

If the Restart System message appears, restart the computer in order for the configuration to take effect. An installation job log named bkupinst.htm is created in the Application Data folder on the computer where Backup Exec is installed. This file lists any errors that may have occurred during installation. The last line of the log indicates if the installation was successful and if you must restart the computer.

After you install Backup Exec on the media server, Backup Exec Agent software can be installed and configured on remote servers over the network.

Before Starting Backup Exec

For best results before starting Backup Exec, review the following guidelines.

Note: For more detailed information on the below topics, see the ***Symantec Backup Exec for Windows Servers Administrator's Guide***.

- Make sure your storage devices are connected and configured properly.
- Decide if your backup will be to a tape device or a disk device. You can configure both devices when you prepare your Backup Exec environment.
- If you're backing up to a tape device, verify that the device is supported. You can install drivers for the devices when you configure your Backup Exec environment.
- If you're backing up to a disk device using the Backup-to-Disk feature, decide where you can create a backup folder. You should create it on a disk that won't be included in the backup jobs and that has enough free space to contain the backup job.
- Understand how Backup Exec provides overwrite protection for your media.

- Understand the default media set and its infinite overwrite protection period.
- Learn about creating new media sets with weekly, monthly, or quarterly retention periods.
- Decide what Windows credential you want your Backup Exec logon account to use when browsing and making backup selections. You can use an existing account, or create a new one. You'll be prompted for a default Backup Exec logon account when you configure your Backup Exec environment.
- Decide the format that you want to display all reports, either HTML or Adobe Portable Document Format (PDF). The default setting is HTML.

Initial Backup Exec Server Configuration

To start the Backup Exec Administration Console, click **Start** > **All Programs** >**Symantec Backup Exec for Windows Servers**.

The first time BackupExec Administration Console is run, the Getting Started with Backup Exec page appears. This page provides a series of wizards that you can follow to configure environment settings in Backup Exec, including logon accounts, devices, and media sets. Also, you can access the Backup Exec Assistant, which has links to additional wizards, documentation, and technical support assistance or you can create a backup job by using the Backup Wizard.

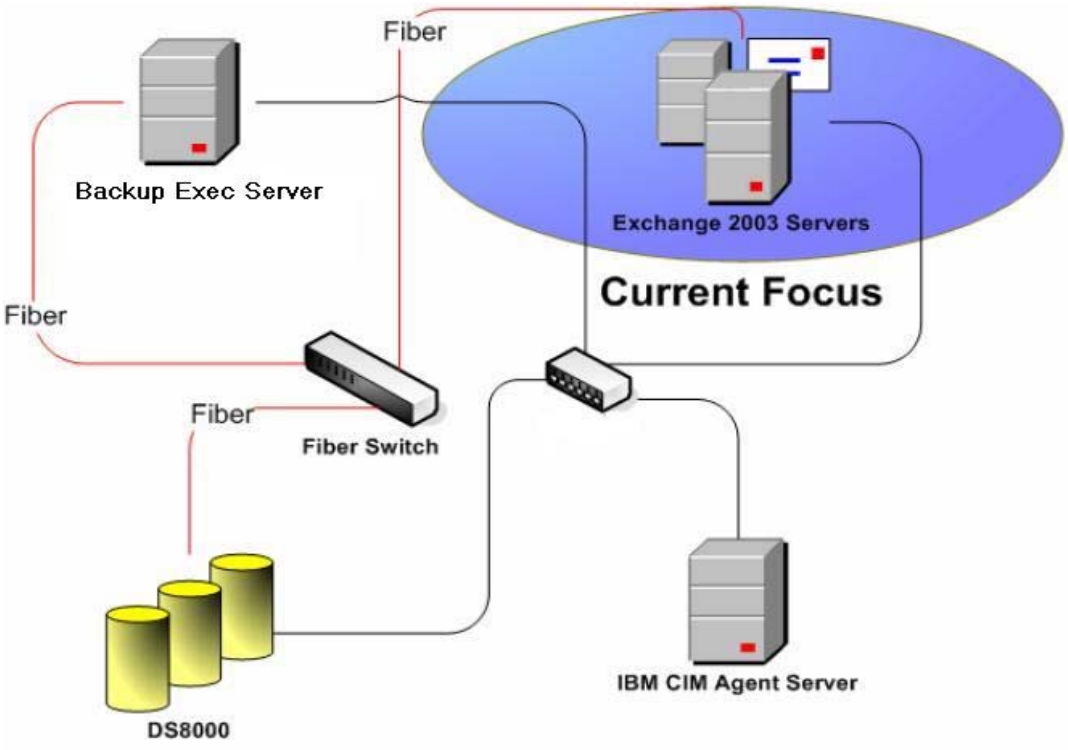
If you do not use the Getting Started with Backup Exec page, you can use the default logon account and media set. The Backup Exec defaults are created during the installation of Backup Exec. The default logon account credentials match the credentials provided during the installation of Backup Exec. The default media set is Keep Data Infinitely - Do Not Allow Overwrite with append and overwrite protection periods set to Infinite. However, you cannot create a backup job until you configure a device.

To access the Getting Started with Backup Exec page, Click **Help** > **Getting Started**.

NOTE: After installation completes, and before pushing out remote agents, run the Symantec Live Update to apply the latest Backup Exec patches. Critical patches for VSS operations include Hotfixes 2, 6, and 11.

Installing the Remote Agent for Windows Systems

After the Backup Exec Media Server is configured, the Remote Agent for Windows Systems must be pushed out to the Exchange servers you intend to backup. The Exchange Agent, installed on the Backup Exec Media server, communicates with the Remote Agent for Windows Systems to manage Exchange server backups.



To install the Remote Agent for Windows Systems on remote servers:

1. On the Backup Exec Server, go to Add/Remove Programs. Click on the **Change** button for Symantec Backup Exec for Windows Servers.
2. Uncheck **Local Install**, check the **Remote Install**.
3. Right click on **Windows Remote Agents**, and select **Add Remote Computer**
4. Select the target computer from the list, and enter the appropriate account credentials.
5. Select the Remote Agent for Windows Systems, and set it to install.
6. Verify the correct Backup Exec Media Server is listed, and click **OK**

7. Click **Next**. A summary of install options appears, click **Install** to proceed. A status window appears, with installation summary. Click **Finish** after validating installation was successful.

Information for Microsoft Exchange Cluster Environments

In addition to the local installation requirements, the following points apply to cluster installations:

- The Remote Agent for Windows Systems is installed on each node of the Exchange cluster. Once installed, the Agent is cluster aware and will recognize and manage the Exchange virtual server backups (EVS)
- Any subsequent Symantec patches or Hotfixes must be applied to the Media server, then pushed out by Remote Agent to each individual node.
- The Backup Exec Continuous Protection Server does not currently support Exchange clusters, this support is planned for a future release.
- When configuring backup jobs, select the Exchange virtual server name (EVS) rather than the Exchange node name.

Exchange Backup and Restore

Overview of the Backup Exec Agent for Exchange

Symantec™ Backup Exec 11d for Windows Servers - Agent for Exchange Server redefines traditional Exchange data protection, minimizing daily Exchange backup windows with VSS-based backups. Backup Exec 11d eliminates slow, arduous mailbox level backups, while still enabling the recovery of individual emails, folders, and mailboxes.

Key Benefits

- Helps safeguard critical Microsoft Exchange 2000, 2003, and 2007 Server data. As previously noted, please see the Symantec website for feature support for Exchange Server 2007.
- Minimizes daily backup windows for Exchange with VSS-based backups.
- VSS off-host snapshot backups minimize impact on production Exchange servers.
- Eliminates slow and error prone mailbox “brick level” backups.
- Recovers individual email messages, mailboxes, and public/private folders from database backups—without mailbox level backups—in seconds.

Traditionally, this protection is primarily accomplished through online backups of the Exchange databases. If organizations also need to recover individual email messages or mailboxes, separate slow, error-prone, “brick-level” mailbox backups are typically required to recover these individual items without restoring the entire Exchange database.

Granular Recovery Technology Benefits

The main benefits of Backup Exec’s Granular Recovery Technology (GRT) include:

- Eliminate separate, slow individual mailbox backups completely.
- Perform fast single-pass VSS backups of Exchange databases and still recover individual mailboxes, individual messages, and private and public folders. **NOTE**: For VSS, this feature currently only supports On-host backups. Support for GRT from off-host VSS backups is planned for a future release.
- Works with or without the need for recovery storage groups (RSGs)
- Cut backup time and storage in half by performing fast, single-pass Exchange database backups
- Reduce storage/media costs
- Enable granular recovery or complete database recovery of all Exchange data

With Backup Exec 11d GRT-enabled backups, Exchange mail messages, mailboxes, and folders are restored individually without having to restore the entire Exchange database—and without mailbox level backups. All that is required is a single-pass full or incremental backup of Exchange, including VSS snapshots, so this feature dramatically decreases the time required to back up mailboxes while also reducing the storage requirement. You can now recover critical Exchange data in seconds, including individual emails, individual mailboxes, public folders, calendars, and contacts from a fast, single-pass Exchange database backup.

Performing Exchange VSS Backups

The Exchange Agent supports the Microsoft Volume Shadow Copy Service (VSS), a snapshot provider service that is only available on Windows Server 2003 or later. Using VSS, a point in time view of the Exchange database is snapped and then backed up, leaving the actual Exchange database open and available for users.

Offhost backups are also supported, which offloads the backup and integrity check processing to a Backup Exec media server instead of the Exchange server. Moving the backup load from the Exchange server to a media server enables better backup performance and frees the Exchange server as well.

The Exchange Agent snapshot does **not** support:

- NAS configurations
- The Exchange 2003 Recovery Storage Group feature
- Exchange 2000 on Windows Server 2003. To avoid errors, Symantec recommends that you create a separate, non-snapshot backup job for the Exchange 2000 Server or Exchange Server 2003 on Windows 2000.
- Backup of the Site Replication Services (SRS)
- Mixing snapshot backups and non-snapshot backups is not recommended, due to a Microsoft Exchange limitation. It is possible to run legacy backups, and VSS backups separately in the same environment, however they are not restore compatible. For example, you can not restore a legacy incremental backup over a VSS full backup.
- Backup jobs for which the option **Continuously back up transaction logs with Backup Exec Continuous Protection Server** is enabled.

Before configuring a VSS backup job, set the VSS defaults from the Backup Exec Administration console.

Set the Default VSS Options

1. Set the **Advanced Open File Option** defaults from the Tools menu. Click **Options,** then on the Properties pane, under Job Defaults, click **Advanced Open File**.
2. Select **Use Advanced Open File Option.**
3. Do not enable **Automatically select open file technology.** We must be able to specify which VSS components are used during the backup.

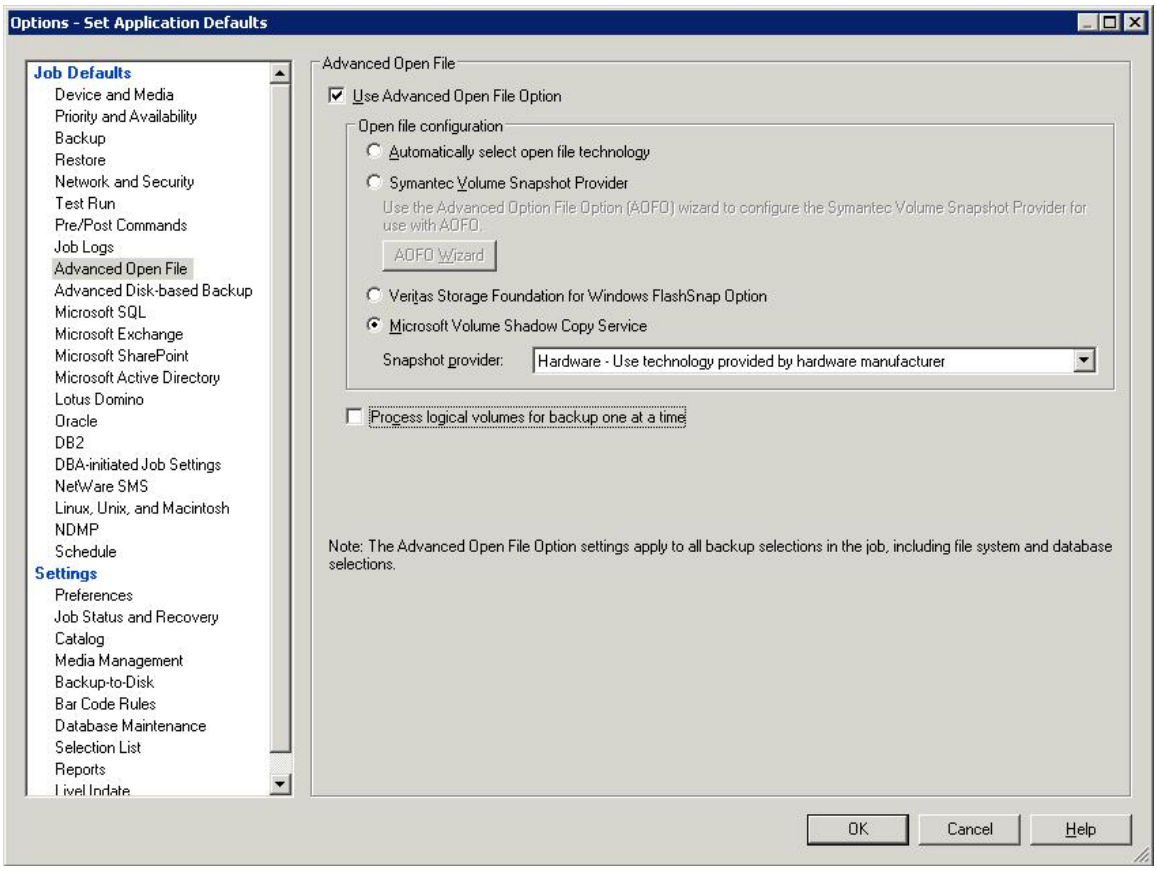


Figure 16: Set Application Defaults window

4. Select **Microsoft Volume Shadow Copy Service**.
5. Under Snapshot provider, select **Hardware – Use technology provided by hardware manufacturer**. This directs the backup to use the IBM Hardware Provider.
6. Do not enable **Process logical volumes for backup one at a time**. The IBM Hardware Provider is capable of capturing snapshots of all volumes in the backup job simultaneously.
7. Click **OK** to save the default settings.

Once the VSS defaults are set, you are ready to configure VSS backup jobs. The following steps walk you through setting up the backup job.

Configure the Backup Job

1. On the navigation bar, click the arrow next to Backup.
2. Click **New Backup Job**.
3. On the Properties pane, under Source, click **Selections**.
4. To view the Exchange data that you want to back up, Expand **domains** > **Active Directory domains** > **Domain Name** > and the Exchange virtual server name.
5. Expand the **Microsoft Information Store** icon, and then select the individual storage groups.

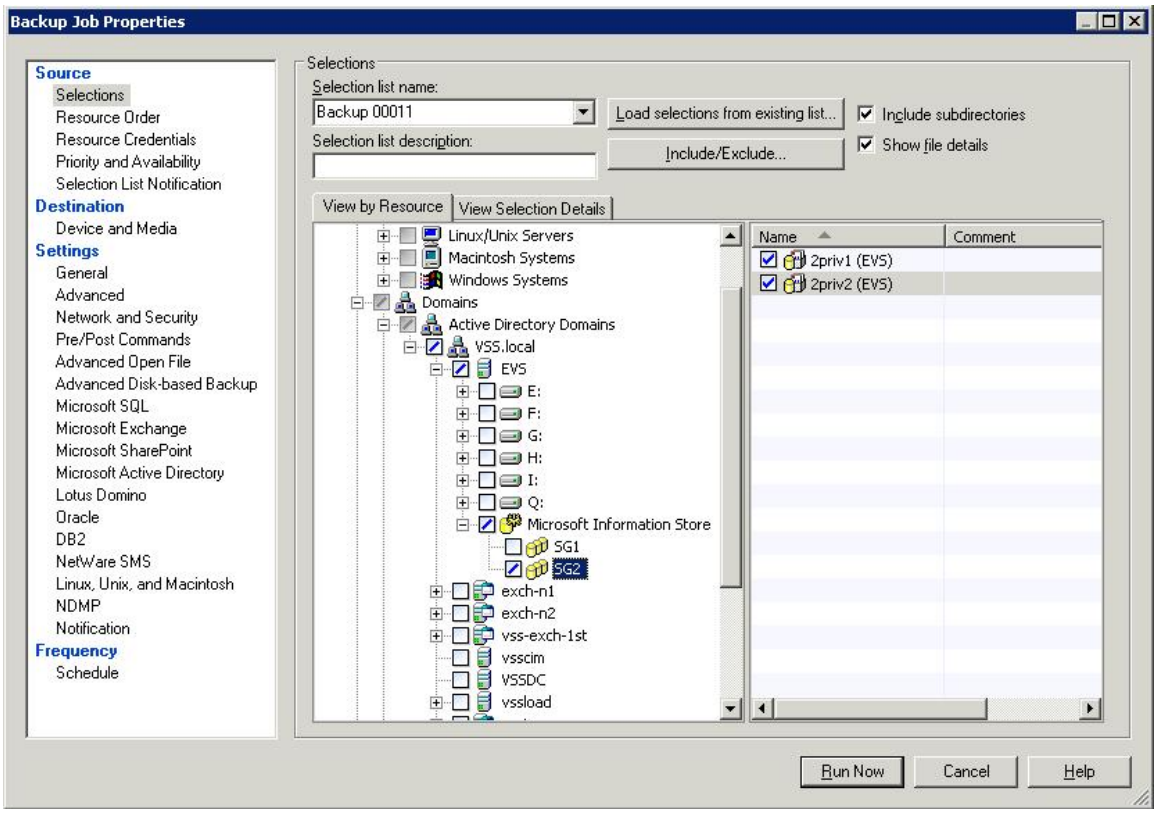


Figure 17: Configuring a backup job

6. If prompted, select a logon account that you can use to connect to the Exchange Server.
7. On the Backup Job Properties pane, under Settings, click **Microsoft Exchange**.

8. Select the appropriate backup method. The following are available backup methods for snapshot backups:

   Exchange 2003

   - Full
   - Copy

   Exchange 2003 with Service Pack 1 or later:

   - Full
   - Copy
   - Differential
   - Incremental

9. Do not enable **Continuous Protection Server**. This is not supported for VSS backups or Exchange clustering.

10. Check **Enable the restore of individual mail messages and folders from Information Store backups** to enable the restore of individual mail messages and folders from full or copy backups of the Information Store.

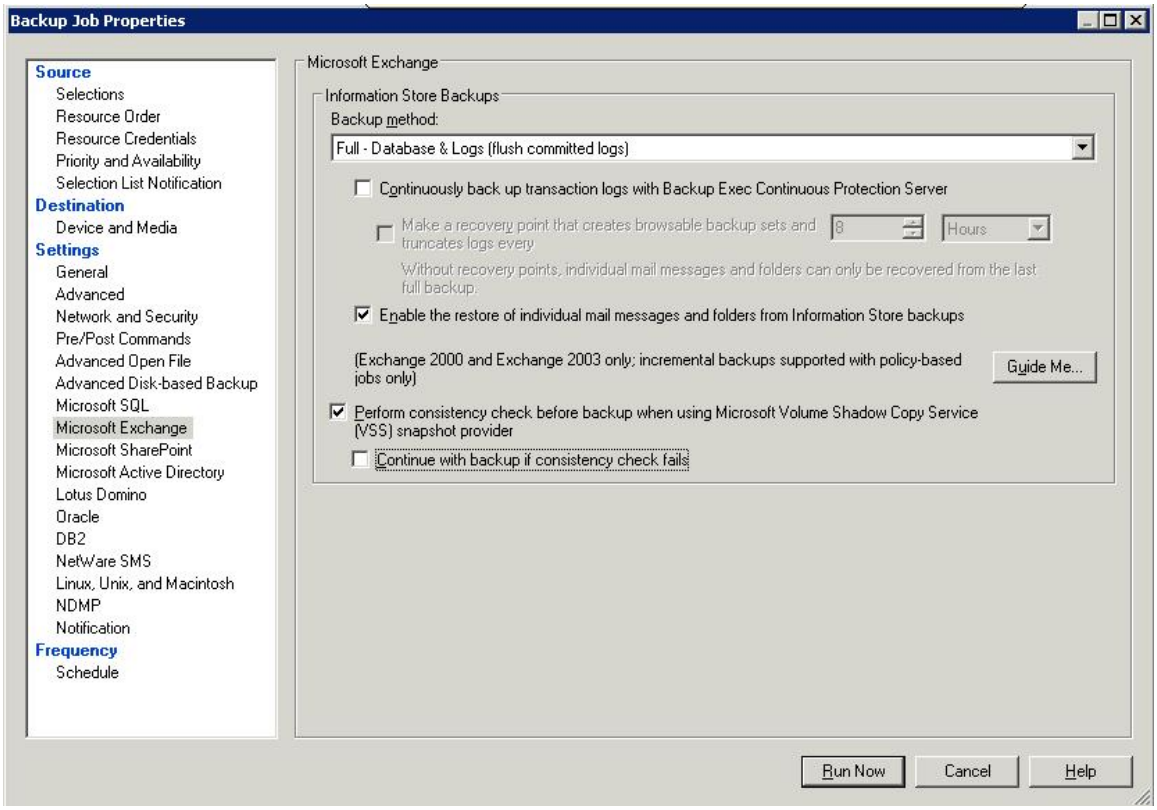


Figure 18: Configuring the backup method

11. Select **Perform consistency check before backup** when using Microsoft Volume Shadow Copy Service (VSS) snapshot provider. Symantec recommends that you perform consistency checks before running snapshot backups.
12. Do not check **Continue with backup if consistency check fails**.
13. Click **Run Now** or go to **Frequency > Schedule** in the left pane to schedule the job.
14. Schedule or start the backup job.

After a VSS backup job is completed, check the section **Backup Set Detail Information** in the job log to make sure **Advanced Open File** was used during the backup.

Exchange Off-Host VSS Backups

Offhost backup enables Backup Exec to move backup processing from the host computer, which is the remote computer that contains the volumes selected for backup, to the Backup Exec media server. The offhost backup creates a snapshot of the volume or volumes that are selected for backup on the remote computer. The snapshots are then imported to the media server, where they are backed up.

The following requirements must be met to use offhost backup.

Media server:

- Backup Exec for Windows Servers version 10.0 or later
- Backup Exec Advanced Disk-based Backup Option
- Backup Exec Advanced Open File Option
- Agent for Exchange

Exchange Server:

- Backup Exec Remote Agent for Windows Servers version 10.0 or later

Media server and the Exchange Server:

- Microsoft Windows Server 2003, Standard, Datacenter, or Enterprise with Service Pack 1 (or later)
- Most recent Volume Shadow Copy Services (VSS) patches.

- A Microsoft VSS hardware provider. Otherwise, the snapshots of the volumes cannot be imported to the media server (transportable shadow copies).
- Ability to access disks that are shared between the media server and the Exchange server.

Configuring an Offhost backup

You can set the offhost backup options for each backup job, or you can set defaults that are used for every backup job.

1. To access offhost backup options for a single backup job:
    a. On the navigation bar, click the arrow next to **Backup**.
    b. Click **New Backup Job** (or open an existing scheduled job)
    c. On the Properties pane, under Settings, click **Advanced Disk-based Option**.
2. To access offhost backup options for all backup jobs:

    On the **Tools** menu, click **Options**. On the Properties pane, under Job Defaults, click **Advanced Disk-based Backup Option**.

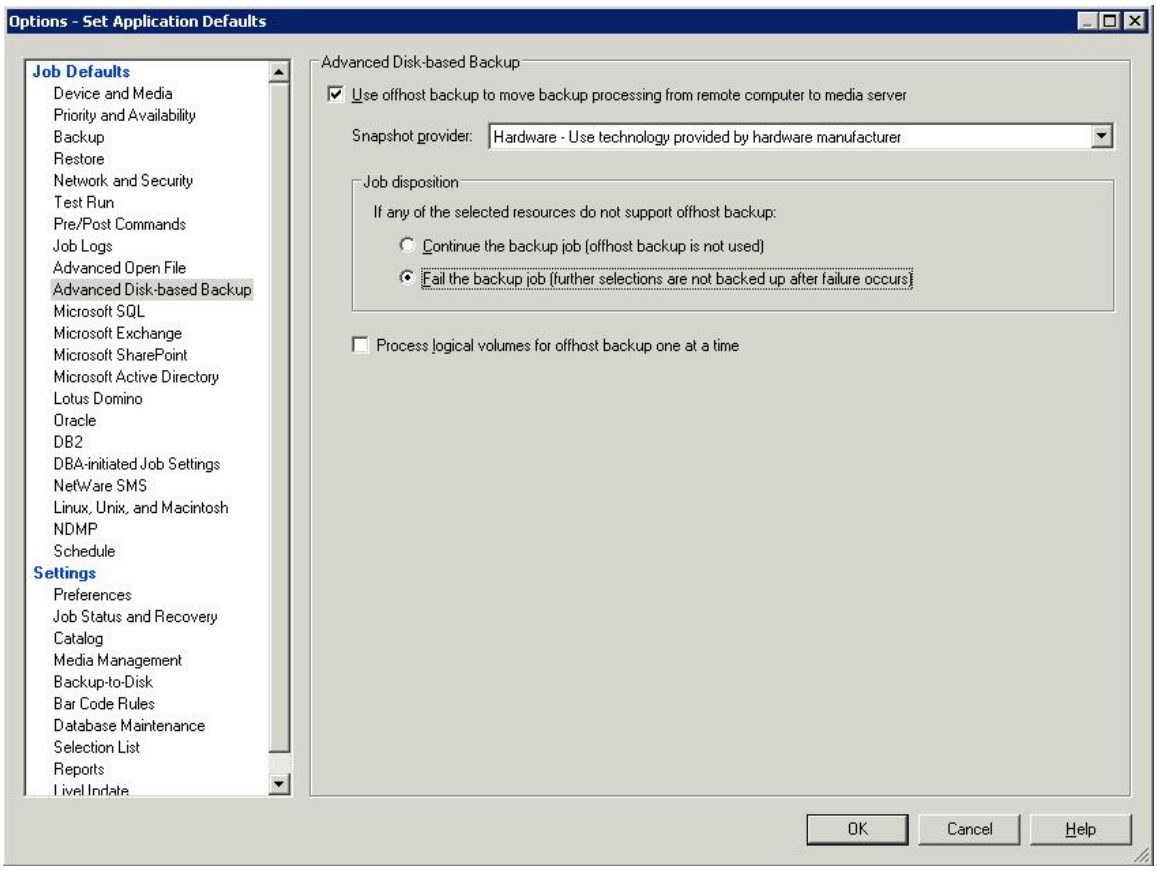


Figure 19: Set Application Defaults window

3. Select **Use offhost backup to move backup processing from remote computer to media server**.
4. Under Snapshot Provider, choose **Hardware - Use technology provided by hardware manufacturer**.
5. Under Job Disposition, select **Fail the backup job**. This option halts the backup if it is unable to use the offhost method.
6. Clear the checkbox **Process logical volumes for offhost backup one at a time**.
7. Click **OK** if you are setting the default values. If you are setting properties for a specific backup job, click **Run Now** or schedule the backup.

NOTE: When performing off-host VSS backups, the backup will go to a .BKF file on the Backup Exec Media server (compared to an IMG file with on-host VSS backups).

Best Practices for Using Offhost Backup

- Keep source volumes and snapped volumes from sharing the same physical disks. If this is not maintained, then any attempt to split the snapshot volume from the original volume fails.
- If the Central Admin Server Option (CASO) is installed, for jobs that use offhost backup, you must manually select the destination device that will run the job rather than allowing the job to be delegated by the central administration server. Otherwise, the job could be delegated to a media server that does not have offhost capability.

Restoring from an Exchange VSS Backup

This procedure details how to select restore job properties for Exchange, and provides definitions for restore options specific to Exchange. For details on how to create a restore job, and for definitions of all other restore properties, see “Restoring data” on page 483 of the Backup Exec Administrators Guide.

Use either the Exchange System Manager utility to manually dismount any databases that are being restored, or check **Dismount database before restore** when creating the restore job.

To restore Exchange data:

1. On the navigation bar, click the arrow next to **Restore**.
2. Click **New Restore Job**.
3. On the **Properties** pane, under **Source**, click **Selections**.
4. In the restore selections list, select the backup sets that you want to restore. Select the Storage Group you want to restore. For information about restoring specific data, see “About restoring Exchange data” on page 1256 of the Backup Exec Administrators Guide.
5. On the Properties pane, under Settings, click **Microsoft Exchange**. Select the appropriate options for your environment and restore objectives. Note that Backup Exec will always do a “no loss restore” with VSS. The existing log files are not deleted, which results in Exchange replaying both existing and restored transaction logs.

   NOTE: If the existing log files are manually deleted before starting the restore job, then it becomes a “point in time” restore, which restores to the state databases and logs were in at time of VSS backup.

6. To enter the path, on the Restore Job Properties pane, under Settings, click **Advanced**, and then enter a path in **Path on media server for staging temporary restore data when restoring individual items from tape**. For more information about this path, see “Advanced options for restore jobs” on page 494 of the Backup Exec Administrators Guide.

7. Select specific restore options from the Properties pane as appropriate, and then start the restore job.

Restrictions when Restoring from Snapshot Backups

Note the following when restoring Exchange data from snapshot backups:

- The specific options **No loss restore**, **Temporary location for log and patch files, Purge all files,** and **Commit after restore completes** are not applicable for VSS. Backup Exec performs a no loss restore and Exchange will use the soft-recovery process when the restored databases are mounted.

- Backup Exec always performs a “no loss” restore from VSS backups. During Exchange recovery, both existing and restored transaction logs will replay. However, as a work around, a “point in time” restore from VSS is possible by manually deleting all current transaction log files before starting the restore job. Point in time restore capability is planned for a future release.

- Exchange 2003 does not support restoring from a snapshot backup to a Recovery Storage Group (RSG).

- Backup Exec 11d does not currently support VSS restores at the Exchange database level. This will be supported in a future release. If restores of individual databases are required, then each Storage Group must be configured with only one database.

Recovering Mailbox Data with Granular Restore Technology

Symantec’s GRT solution provides restore capabilities from any type of Backup Exec backup jobs, including VSS on host snapshot backups. GRT is not currently available from off-host VSS backups. If you checked **Enable the restore of individual mail messages and folders from Information Store backups** on the backup job properties for the Information Store backups, then you can restore individual messages and folders from that backup. The below illustration shows the granular selection possible.

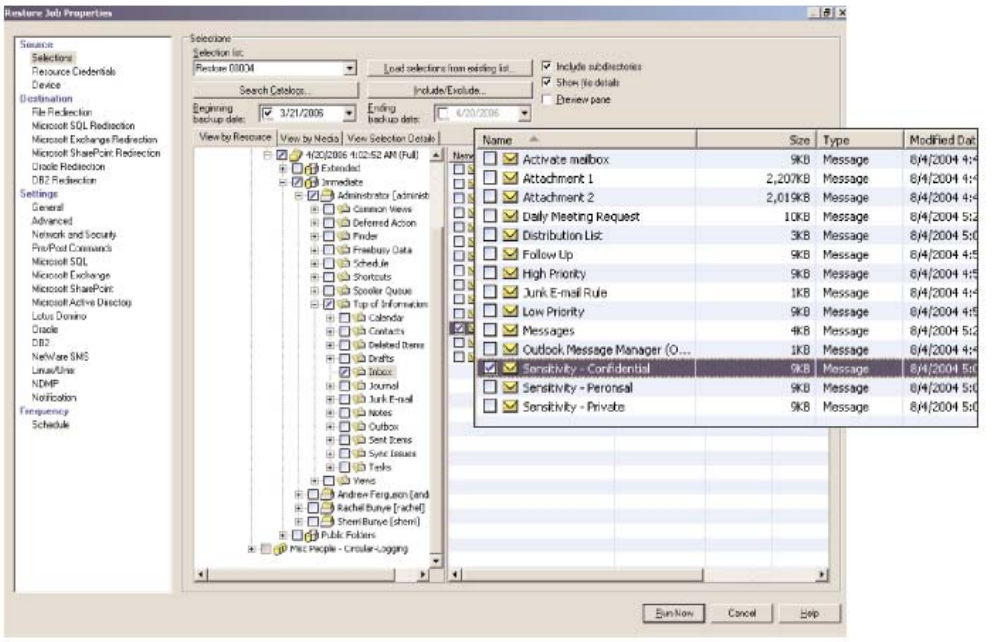


Figure 20: Recovering mailbox data

If you restore individual items from an Information Store backup set that is on a device other than a backup-to-disk folder, then Backup Exec must temporarily stage the entire database to a path on the media server to extract individual items. Because of the potentially large file sizes that are created in the staging location path, system volumes should not be used as a staging location.

To enter the path, on the Restore Job Properties pane, under Settings, click **Advanced**, and then enter a path in **Path on media server for staging temporary restore data when restoring individual items from tape.** For more information about this path, see “Advanced options for restore jobs” on page 494 of the Administrators Guide.

Backup Exec must also have access to a uniquely named mailbox in the Exchange organization. See “Exchange mailbox access requirements” on page 1224 of the Administrators Guide for additional information.

Consistency Checks on Exchange Database and Log Files

For an Exchange VSS backup, Microsoft requires that each database file (.edb, but not .stm) and each transaction log file required for the restore have a checksum consistency check run against the files. This consistency check is accomplished by running **eseutil.exe** with the proper options against the files which exist on the snapshot. For offhost backups, the consistency checks are run on the offhost server rather than on the Exchange Server. Off-loading the consistency check is recommended to further reduce the backup impact on production Exchange servers.

If any of the files fail the consistency check, the entire backup will fail, the backup image will be discarded, and the Exchange VSS Writer will be notified of the failure. When this occurs, Exchange will not truncate log files.

Failure of the consistency check may be an indication of either database corruption or a problem with the snapshot. The Exchange administrator should investigate the reason for the failure by dismounting the Exchange database which caused the failure, and running eseutil.exe against the database file to determine the cause of the corruption.

Best Practices for Exchange Storage and VSS Backups

The following are recommended configurations to prepare the Exchange environment for Backup Exec VSS operations.

- The volume(s) which contains the Exchange databases and log files should be dedicated to Exchange only. Other types of databases (e.g., SQL) should not reside on the volume(s). Only Exchange objects will be included in a snapshot backup.
- Disable circular logging for all Exchange Storage Groups.
- Transaction logs should reside on a different volume than where the Information Store resides.
- If you are running the integrity check, ESEUTIL throttling minimizes the impact on production LUNS during the VSS copy-on-write process. Although the current version of Backup Exec does not provide throttling, this is planned for a future release. It is also recommended to use the offhost feature to further minimize performance impacts.
- If you are planning on restoring individual mailbox messages or folders, you should ensure the backups are to disk, rather than tape. Granular restores from tape require staging of the data from tape to disk first, which impacts the restore times and the ability to meet SLA times.

In order to fully leverage the performance capabilities of the IBM DS8000 and 6000, detailed consideration needs to be given to the logical configuration of the storage units. This is particularly true with I/O intensive applications such as Exchange Server 2003, and even more so when implementing VSS technology.

Volumes intended for VSS use should be created:

- So that source & target volumes are in different ranks
- So that source & target volumes are on the same RIO loop
- So that source & target volumes are managed by different DA pairs
- So that overall system usage is balanced, eliminating 'hot-spots'

Minimizing application impact

- Host-based striping can further reduce latency
- Backup should occur when applications are least active
- Volume creation & storage sizing for maximum Exchange performance should follow published Microsoft guidelines. Contact Microsoft for further information.
- For additional information on configuring your IBM DS8000 for maximum performance, please refer to the IBM System Storage DS8000 Series: Performance Monitoring and Tuning Redbook, which can be found at

http://www.redbooks.ibm.com/abstracts/sg247146.html?Open

Conclusion

The system configurations described here, constructed jointly by IBM and Symantec, and reviewed by Microsoft, are designed to address demanding enterprise requirements for highly available email servers running Microsoft Exchange. Microsoft VSS technology is designed to enable consistent point-in-time copies of Exchange databases, while Transportable Shadow Copies affords the benefit of shifting the task of executing **Eseutil** consistency checking to another server. Both of these features help reduce the traditional backup load on production Exchange servers.

IBM servers and storage systems are designed to provide the processing throughput and storage needed for large user populations. Symantec Backup Exec software is designed to alleviate the complexities of protecting Exchange, while eliminating the traditional daily Exchange backup window. This hardware and software combination forms a high availability platform for mission critical email servers.

Appendix

Solution Component Information

Hardware Configuration

Host Configuration

Exchange 2003 Servers

- Server type: 4 x Intel Xeon 2.8 GHz 4096 MB RAM
- Operating System: Microsoft Windows 2003 Enterprise Edition SP1

Exchange Client / Loadsim

- Server type: 1 x Intel Xeon 2.8 GHz 1024 MB RAM
- Operating System: Microsoft Windows 2003 Enterprise Edition SP1

Backup Exec Media Server

- Server type: 1 x Intel Xeon 2.4 GHz 1024 MB RAM
- Operating System: Microsoft Windows 2003 Enterprise Edition SP1

IBM DS CIM Server (ICAT)

- Server type: 1 x Intel Xeon 2.8 GHz 1024 MB RAM
- Operating System: Microsoft Windows 2003 Enterprise Edition SP1

HBA Configuration

- Exchange and Backup Exec servers contained one dual-port Qlogic A2462 HBA
- Driver version: Storport 9.1.2.19
- Bios: 1.12
- Firmware: 4.00.23
- SDDDSM Version: 2.1.1.1-1

Storage Subsystem Configuration

Logical Configurations

dscli> lsrank -l

Date/Time: February 6, 2007 8:48:39 AM PST IBM DSCLI Version: 5.1.600.248 DS: IBM.2107-75DGTN1

ID	Group	State	datastate	Array	RAIDtype	extpoolID	extpoolnam	stgtype	exts	usedexts
R0	0	Normal	Normal	A0	5	P0	fb_ext_pool0	fb	779	92
R1	0	Normal	Normal	A1	5	P0	fb_ext_pool0	fb	779	280
R2	0	Normal	Normal	A2	5	P0	fb_ext_pool0	fb	779	88
R3	0	Normal	Normal	A3	5	P0	fb_ext_pool0	fb	779	88
R4	1	Normal	Normal	A4	5	P1	fb_ext_pool1	fb	909	320
R5	1	Normal	Normal	A5	5	P1	fb_ext_pool1	fb	909	120
R6	1	Normal	Normal	A6	5	P1	fb_ext_pool1	fb	909	120
R7	0	Normal	Normal	A7	10	P2	VSS_extpool_R7_4+4_p2	fb	519	200
R8	1	Normal	Normal	A8	10	P3	VSS_extpool_R8_3+3_p3	fb	388	60
R9	0	Normal	Normal	A9	10	P4	VSS_extpool_R9_4+4_p4	fb	519	200
R10	1	Normal	Normal	A10	10	P5	VSS_extpool_R10_3+3_p5	fb	388	150
R11	0	Normal	Normal	A11	10	P6	VSS_extpool_R11_4+4_p6	fb	519	200
R12	1	Normal	Normal	A12	10	P7	VSS_extpool_R12_4+4_p7	fb	519	519
R13	0	Normal	Normal	A13	10	P8	VSS_extpool_R13_4+4_p8	fb	519	0
R14	1	Normal	Normal	A14	10	P9	VSS_extpool_R14_4+4_p9	fb	519	0
R15	0	Normal	Normal	A15	10	P10	VSS_extpool_R15_4+4_p10	fb	519	0

dscli> lsfbvol -volgrp v6

Date/Time: February 6, 2007 9:51:32 AM PST IBM DSCLI Version: 5.1.600.248 DS: IBM.2107-75DGTN1

Name	ID	accstate	datastate	configstate	deviceMTM	datatype	extpool	cap (2^30B)	cap (10^9B)	cap (blocks)
Exdata1	1200	Online	Normal	Normal	2107-900	FB 512	P2	100.0	-	209715200
Exdata2	1201	Online	Normal	Normal	2107-900	FB 512	P2	100.0	-	209715200
Exlog1	1300	Online	Normal	Normal	2107-900	FB 512	P3	30.0	-	62914560
Exlog2	1301	Online	Normal	Normal	2107-900	FB 512	P3	30.0	-	62914560
Quorum	1302	Online	Normal	Normal	2107-900	FB 512	P5	10.0	-	20971520
SMTPQ	1304	Online	Normal	Normal	2107-900	FB 512	P5	20.0	-	41943040

```
dscli> lsfbvol -volgrp v8
Date/Time: February 6, 2007 9:53:33 AM PST IBM DSCLI Version: 5.1.600.248 DS: IBM.2107-75DGTN1
Name    ID   accstate datastate configstate deviceMTM datatype extpool cap (2^30B) cap (10^9B) cap (blocks)
==========================================================================================
VSS_data1 1400 Online   Normal    Normal     2107-900  FB 512   P4         100.0          -   209715200
VSS_data2 1401 Online   Normal    Normal     2107-900  FB 512   P4         100.0          -   209715200
VSS_data3 1402 Online   Normal    Normal     2107-900  FB 512   P6         100.0          -   209715200
VSS_data4 1403 Online   Normal    Normal     2107-900  FB 512   P6         100.0          -   209715200
VSS_log1  1500 Online   Normal    Normal     2107-900  FB 512   P5          30.0          -    62914560
VSS_log2  1501 Online   Normal    Normal     2107-900  FB 512   P5          30.0          -    62914560
VSS_log3  1502 Online   Normal    Normal     2107-900  FB 512   P5          30.0          -    62914560
VSS_log4  1503 Online   Normal    Normal     2107-900  FB 512   P5          30.0          -    62914560
```

Switch Configuration

- Switch Type: IBM 2109 F16
- Fabric OS: v3.1.2a
- Made on: Wed Mar 31 21:16:31 PST 2004
- Flash: Wed Mar 31 21:17:22 PST 2004
- BootProm: Tue Oct 30 10:24:38 PST 2001

Software Configuration

Exchange 2003 Configuration

- The version of Exchange 2003 was 2003 Enterprise Edition version 6.5.7638.2, service pack 2.
- The Microsoft Exchange Server 2003 Load Simulator was version 6.5.7618.0.

Windows Server

- Windows 2003 Enterprise Edition Server, SP1

Backup Client Software Configuration

- Symantec Backup Exec 11d Remote Agent for Windows

Backup Server Configuration

- Symantec Backup Exec 11d for Windows Servers

The following Backup Exec optional components ***must*** be installed

- Advanced Open File
- Advanced Disk-based Backup
- Exchange Agent

VDS/VSS Provider Configuration

- Provider name: 'IBM Hardware Provider for VSS'
- Provider type: Hardware
- Provider Id: {d90dd826-87cf-42ce-a88d-b32caa82025b} version: 2.4.4.0828

DS8000 DSCLI Configuration

DS command line interface software version 5.1.600.248 was installed on the IBM CIM server.

IBM DS CIM (ICAT) Configuration

Version 5.1.0.50 was installed on the IBM CIM server.

Microsoft Hotfixes and Patches

The following table is a complete list of Microsoft hotfixes and patches applied to each Exchange Cluster node and backup server:

KB890046	KB891957	KB893756	KB896358	KB896424	KB896428
KB898715	KB898790	KB899587	KB899588	KB899589	KB899591
KB900725	KB901017	KB901214	KB902400	KB903650	KB904706
KB905414	KB908519	KB908521	KB908531	KB910437	KB911280
KB911562	KB911564	KB911567	KB911897	KB911927	KB912919
KB913648	KB914388	KB914389	KB916048	KB916281	KB917159
KB917344	KB917422	KB917537	KB917734	KB917953	KB918118
KB918439	KB918899	KB920213	KB920214	KB920670	KB920683

KB920685	KB921398	KB921883	KB922582	KB922616	KB922760
KB922819	KB923191	KB923414	KB923689	KB923694	KB923980
KB924191	KB924496	KB924667	KB925398	KB925454	KB925486
KB925876	KB926436	KB928090	KB928255	KB928388	KB928843
KB929120	KB929969	KB931836	Q147222		

[i] davwest@us.ibm.com, IBM Systems & Technology Group

[ii] dhartma@us.ibm.com, IBM Systems & Technology Group